NISTIR 4659

Glossary of Computer Security Terminology

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4659

Glossary of Computer Security Terminology

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, MD 20899

September 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents a glossary of computer security terminology, whose development was sponsored under the auspices of the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This glossary is a collection of terms and definitions used by various federal departments and agencies in their policies, standards, and other publications. This glossary did not seek to arrive at a single agreed-upon definition of each entry; therefore, some definitions may not be wholly consistent. Although never formally issued by the NSTISSC, since the document does reflect actual usage of these terms, it may provide a useful reference source to the computer security practitioner.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this glossary. However, as this material may be of use to other organizations, it is being reprinted by NIST to provide for broad public dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the Subcommittee on Information Systems Security (SISS) and the Executive Secretariat of the National Security Telecommunications and Information Systems Security Committee for their kind permission to publish this report. We also wish to acknowledge the many computer security professionals who participated in the development of this glossary.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

Glossary of Computer Security Terminology

- A -

aborted connection	Disconnection which does not follow established procedures. This may occasionally result from a bad phone connection, but more typically results when the user "hangs up" without attempting to issue the disconnect commands. Note: Some systems are sensitiue to aborted connections, and do not detect the disconnect and reset for the next user. Continued aborts are considered [improper], and may result in a warning or revocation of access privileges. (BBD)
acceptable level of risk	A judicious and carefully considered assessment by the appropriate designated approving authority (DAA) that an automatic data processing (ADP) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of ADP assets; threats and vulnerabilities; countermeasures and their efficacy in compensating for vulnerabilities; and operational requirements. (OPNAVINST 5239.1A)
acceptance	Indicates a facility or system generally meets technical and performance standards but may have minor exceptions which do not keep the facility from meeting operational and security requirements, (AFR 700-10)
acceptance inspection	The final inspection to determine if a facility or system meets the specified technical and performance standards. It is held immediately after facility and software testing and is the basis for commissioning or accepting the information system. The results are documented on AF Form 1261, Information Systems Acceptance, Commissioning, and Removal Certificate. (AFR 700-10)
access	1) A specific type of interaction between a subject and an object that results in the flow of information from one to the other. (DOD 5200.28-STD; AR 380-380; DCID 1/16, Sup.)

2) The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system or network. (DCID 1/16; DOD 5200.28M)

3) A specific type of interaction between a subject (i.e., person, process or input device) and an object (i.e., an AIS resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information.(DODD 5200.28)

4) The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any resource of an ADP system. (FIPS PUB 39)

5) The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system. Personnel only receiving output products from the ADP system and not inputting to or otherwise interacting with the system (i.e., no "hands on" or other direct input or inquiry capability) are not considered to have ADP system access and are accordingly not subject to the personnel security requirements. Such output products, however, shall either be reviewed prior to dissemination or otherwise determined to be properly identified as to content and classification. (OPNAVINST 5239.1A; AFR 700-10)

6) A user's ability to communicate with (input to or receive output from) a system or to have entry to a specified area. (AFR 205-16)

access category

One of the classes to which a user, program or process in an ADP system may be assigned on the basis of the resources or groups of resources that each is authorized to use. (AR 380-380; FIPS PUB 39)

access control

1) The process of limiting access to the resources of a system to authorized users, programs, processes or other systems (in networks). (AR 380-380)

	2) The process of limiting access to information or to resources of an ADP system to only authorized users. (DOE 5637.1) 3) The process of limiting access to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks. (FIPS PUB 39) 4) Synonymous with CONTROLLED ACCESS and CONTROLLED ACCESSIBILITY.
access control list	A list of subjects which are authorized to have access to some object. (MTR-8201)
access control measures	Hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these designed to detect or prevent unauthorized access to an ADP system and to enforce access control. (DOE 5637.1)
access control mechanism(s)	Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to an automated system. (AR 380-380; FIPS PUB 39)
access control roster	***A list of human and computer users who communicate or interface with a system, that documents the degree of access and control for each user. (AFR 205-16)***
access level	***1) The hierachical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. (NCSC-TG-004-88)*** 2) See SECURITY LEVEL, CATEGORY, and SENSITIVITY LABEL.
access list	A catalogue of users, programs, or processes and the specifications of access categories to which each is assigned. (AR 380-380; FIPS PUB 39)
access mode	A distinct operation recognized by the protection mechanisms as a possible operation on an object. Read, write and append are possible modes of access to a file, while execute is an additional mode of access to a program. (MTR-8201)

access password	A password used to authorize access to data and distributed to all those who are authorized similar access to that data. (FIPS PUB 112; ***AFR 205-16***)
access period	A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail. (FIPS PUB 39)
access port	A logical or physical identifier that a computer uses to distinguish different terminal input/output data streams. (CSC-STD-002-85)
access to information	The function of providing to members of the public, upon their request, the government information to which they are entitled under law. (A-130)
access type	The nature of an access right to a particular device, program, or file (such as read, write, execute, append, modify, delete, and create). (AR 380-380; FIPS PUB 39)
accountability	1) The quality or state which enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible. (FIPS PUB 39; AR 380-380) 2) The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions. (DODD 5200.28; DOE 5637.1) ***3) The property that allows system activities to be traced to the responsible individuals. (AFR 205-16)***
accountability information	A set of records, often referred to as an audit trail, that collectively provide documentary evidence of the processing or other actions related to the security of an ADP system. (DOE 5637.1)
accreditation	***1) Official authorization, by the DAA, to place an automated system into operation. This authorization is a statement that the level of residual risk is sufficiently low to allow operation for a specified use. Accreditation is site specific and dependent on meeting local security measures and procedures. See "Approval to Operate". (AFR 205-16)***

2) The official authorization granted to an information system to process sensitive information in its operational environment based on comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel and communications security controls. (AFR 700-10)

3) The authorization and approval granted to a system or network to process classified or sensitive data. Accreditation will be made on the basis of certification by a competent authority that designated technical personnel have verified that specified technical requirements for achieving adequate data security have been met. (AR 380-380)

4) A formal declaration by the responsible SOIC, or his designee, as appropriate, that the ADP system or network provides an acceptable level of protection for processing and/or storing intelligence information. An accreditation should state the operating mode and other parameters peculiar to the ADP system or network being accredited. (DCID 1/16, Sup.)

5) The formal declaration by a designated official that an automated information system or network is approved to operate: in a particular security mode; with a prescribed set of technical and nontechnical security safeguards; against a defined threat; in a given operational environment; under a stated operational concept; with stated interconnections to other automatic information systems or networks; and at an acceptable level of risk for which the accrediting official has formally assumed responsibility. The accreditation statement affixes security responsibility with the accrediting official and shows that due care has been taken for security. (DOE 5637.1)

6) The authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. (FIPS PUB 39)

7) A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (DODD 5200.28)

8) A policy decision by the responsible DAA resulting in a formal declaration that appropriate security countermeasures have been properly implemented for the ADP activity or network, so that the activity or network is operating at an acceptable level of risk. The accreditation should state the mode of operation and any operating limitations applicable to the ADP activity or network. (OPNAVINST 5239.1A)

10) See APPROVAL TO OPERATE and APPROVAL/ ACCREDITATION.

accreditation authority

1) An official designated to accredit systems for the processing, use, storage, and production of sensitive defense material. (AR 380-380)

2) See DESIGNATED APPROVING AUTHORITY.

AC erasure

The remnant or residual signal level after erasure with electrical degaussing equipment that should measure 90 decibels (dB) below saturated signal level. New equipment should be selected to meet the 90 dB standard. (AFR 205-16)

acoustic emanation

A signal transmitted mechanically via vibrations in either the air or some other conducting medium. (NACSEM 5106)

active wiretapping	The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false signals, or by altering the communications of legitimate users. (FIPS PUB 39)
activity	A security model rule stating that once an object is made inactive, it cannot be accessed until it is made active again. (MTR-8201)
add-on security	1) The retrofitting of protection mechanisms, implemented by hardware or software, after the ADP system has become operational. (AR 380-380; FIPS PUB 39) ***2) The retrofitting of protection mechanisms, implemented in hardware or software. (NCSC-TG-004-88)***
address space	The virtual memory that can be addressed by a process. The maximum size of a process address space is usually a function of the underlying hardware. (MTR-8201)
ad hoc query	A method which allows the user in a data base environment to dynamically create his own view of the data and the method of retrieval for the information without intervention. (AR 380-380)
administrative security	1) The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide an acceptable level of protection for data. (OPNAVINST 5239.1A; DOE 5637.1; FIPS PUB 39) ***2) The management constraints and supplemental controls established to provide an acceptable level of protection for data. (NCSC-TG-004-88)*** 3) Synonymous with PROCEDURAL SECURITY.
ADP facility	One or more rooms, generally contiguous, containing the elements of an ADP System. (DOE 5637.1)

ADP security	Measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of ADP systems and data, and denial of service to process data. ADP security includes consideration of all hardware/software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the ADP system and for the data or information contained in the system. (OPNAVINST 5239.1A)
ADP security documentation	Documents which describe an activity's ADP security posture and include risk assessment plan and reports, security test and evaluation plans and reports, Inspector General inspection reports and findings, incident reports, contingency plans and test results, and standard operating procedures. (OPNAVINST 5239.1A)
ADP security staff	Individuals assigned and functioning as action officials for ADP security within their respective organization. (OPNAVINST 5239.1A)
ADP storage media	The physical substance(s) used by an ADP system upon which data is recorded. (CSC-STD-005-85)
ADP system	1) The central computer facility and any remote processors, terminals, or other input/output/ storage devices connected to it by communications links. Generally, all of the components of an ADP system will be under the authority of one SOIC or his designee. (DCID 1/16, Sup.) 2) An assembly of components of computer hardware, telecommunications, interconnections with other ADP equipment (e.g., networks), and the entire collection of software that is executed on that hardware. Included in this definition are word processors, microprocessors, personal computers, controllers, automated office support systems (AOSS), or other stand-alone or special computer systems. (DOE 5637.1)

ADP system security	1) Includes all hardware/software functions, characteristics, and features, operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities, and, the management constraints, physical structures, and devices; personnel and communication controls needed to provide an acceptable level of protection for classified material to be contained in the computer system. (DOD 5200.28M) 2) All of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy. (FIPS PUB 39)
Affirm	A formal methodology developed at the University of Southern California Information Sciences Institute (USC-ISI) for the specification and verification of abstract data types, incorporating algebraic specification techniques and hierarchical development. (MTR-8201)
agency	Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget and the Office of Administration. (A-130)
aggregation	***The result of assembling or combining distinct units of data when handling sensitive information. Aggregation of data at one senisitivity level may result in the total data being designated a higher sensitivity level. (AFR 205-16)***

AIS security	1) Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data, and denial of service. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable level of protection for an AIS and for data handled by an AIS. (DODD 5200.28) 2) See COMPUTER SECURITY.
analysis	See COST-ANALYSIS, CRYPTOANALYSIS, and RISK ANALYSIS.
annual loss expectancy (ALE)	The ALE of an ADP system or activity is the expected yearly dollar value loss from the harm to the system or activity by attacks against its assets. (OPNAVINST 5239.1A)
application	Those portions of a system, including portions of the operating system, that are not responsible for enforcing the security policy. (CSC-STD-003-85; CSC-STD-004-85)
application software (functional)	***Routines and programs designed by, or for system users and customers. By using available automated system equipment and basic software, application software completes specific, mission-oriented tasks, jobs, or functions. It can be either general purpose packages, such as demand deposit accounting, payroll, machine tool control, or specific application programs tailored to complete a single or limited number of user functions (base-level personnel, depot maintenance, missile or satellite tracking). Except for general purpose packages that are acquired directly from software vendors or from the original equipment manufacturers, this type of software is generally developed by the user either with in-house resources or through contract services. (AFR 205-16)***

approval/ accreditation	The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls. (DOD 5200.28-STD)
approval to operate	***1) Concurrence by the DAA that minimum security requirements are met and there is an acceptable level of risk. It authorizes the operation of an automated system or network at a computer facility. Approval results from a satisfactory analysis of the computer facility, automated system, and automatic data system certifications and the operational environment of the automated system entity by the DAA. (AFR 205-16)*** 2) See ACCREDITATION.
approved circuit	Synonymous with PROTECTED DISTRIBUTION SYSTEM.
approving authority	See DESIGNATED APPROVING AUTHORITY.
arrest	The discovery of user activity not necessary to the normal processing of data which might lead to a violation of system security and force termination of the processing. (OPNAVINST 5239.1A; AR 380-380; DOD 5200.28M)
assessment	An in-depth study of encrypted text, related traffic and collateral information to determine the adequacy of the technical design and security provided by a code, cipher or other manual cryptosystem. (NACSI 4007)
asset	Any software, data, hardware, administrative, physical, communications, or personnel resource within an ADP system or activity. (OPNAVINST 5239.1A)

assurance	A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation. (DODD 5200.28)
assurance testing	A process used to determine that the security features of a system are implemented as designed, and that they are adequate for the proposed environment. This process may include hands-on functional testing, penetration testing and/or verification. (DOE 5637.1)
asynchronous attack	[An] asynchronous attack [...] is an attempt to exploit the interval between a defensive act and the attack in order to render inoperative the effect of the defensive act. For instance, an operating task may be interrupted at once following the checking of a stored parameter; the user regains control and malevolently changes the parameter; the operating system regains control and [continues] processing using the maliciously altered parameter. (JL)
attack	1) The realization of a threat. How often a threat is realized depends on such factors as the location, type, and value of information being processed. Thus, short of moving the system or facility or radically changing its mission, there is usually no way that the level of protection can affect the frequency of attack. The exceptions to this are certain human threats where effective security measures can have a deterrent effect. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (OPNAVINST 5239.1A)

2) The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. (NCSC-TG-004-88)

attention character

In TCB design, a character that, when entered from a terminal, tells the TCB that the user wants a secure communications path from the terminal to some trusted code, in order to provide a secure service for the user, such as logging in or logging out. (MTR-8201)

audit

1) An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures. (DODD 5200.28)

2) To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

a. Internal Security Audit. An audit conducted by personnel responsible to the management of the organization being audited.

b. External Security Audit. An audit conducted by an organization independent of the one being audited. (OPNAVINST 39.1A; AR 380-380; FIPS PUB 39)

audit trail

1) An automated or manual set of records providing documentary evidence of user transactions. Used to aid in tracing system activities. (AFR 205-16)

2) A chronological record of activities which will enable the reconstruction, review, and examination of the sequence of environments and activities concerning each event in a transaction. (AR 380-380)

3) A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. (DOD 5200.28-STD)

4) A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. (DODD 5200.28; FIPS PUB 39)

5) A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of events leading towards a particular final result. (OPNAVINST 5239.1A)

6) A chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results. (NCSC-TG-004-88)

authenticate

1) To establish the validity of a claimed identity. (DOD 5200.28-STD; JCS PUB 6-03.7)

2) a. To verify the identity of a user, device or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

b. To verify the integrity of data that have been stored, transmitted or otherwise exposed to possible unauthorized modification. (NCSC-TG-004-88)

authentication

1) A means of identifying individuals and verifying their eligibility to receive specific categories of information. (AFR 205-16)

2) The act of identifying or verifying the eligibility of a station, originator, or individual to access information. This measure is designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. (AR 380-380)

3) A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified. (DCID 1/16; DCID 1/16, Sup.)

4) The act of verifying the claimed identity of an individual, station or originator. (DOE 5637.1)

5) a. The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

b. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. (FIPS PUB 39)

6) Measures designed to provide protection against fraudulent transmission and imitative communications deception by establishing the validity of transmission, message, station, or individual. (NCSC-9)

authentication equipment

Equipment designed to provide protection against fradulent transmissions and imitative communications deception or to establish the authenticity of a transmission, message, station, originator, or telecommunications system. (NACSIM 2002)

authentication period

Authentication period is the maximum acceptable period between any initial authentication process and subsequent reauthentication processes during a single terminal session or during the period data is being accessed. (FIPS PUB 112)

authentication process

The actions involving (1) obtaining an identifier and a personal password from an ADP system user; (2) comparing the entered password with the stored, valid password that was issued to, or selected by, the person associated with that identifier; and (3) authenticating the identity if the entered password and the stored password are the same. (Note: If the enciphered password is stored, the entered password must be enciphered and compared with the stored ciphertext or the ciphertext must be deciphered and compared with the entered password.) (FIPS PUB 112)

authentication system

A cryptosystem or a cryptographic process used for authentication. (NCSC-9)

authenticator

1) The means used to identify or verify the eligibility of a station, originator or individual to access specific categories of information. The authenticator may be a symbol, sequence of symbols, or series of prearranged bits that are usually inserted at a predetermined point within a message or transmission for the purpose of authentication. (AR 380-380)

2) a) The means used to identify or verify the eligibility of a station, originator, or individual to access specific categories of information.

b) A symbol, a sequence of symbols, or a series of bits that are arranged in a predetermined manner and are usually inserted at a predetermined point within a message or transmission for the purpose of an authentication of the message or transmission. (FIPS PUB 39)

3) A symbol or group of symbols, or a series of bits selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission. (NCSC-9)

4) The means used to confirm the identity or to verify the eligibility of a station, originator or individual. (NCSC-TG-004-88)

authorization	1) The privilege granted to an individual by a designated official to access information based upon the individual's clearance and need-to-know. (DOE 5637.1) 2) The granting to a user, program, or process the right of access. (AR 380-380; FIPS PUB 39)
authorization process	The actions involving (1) obtaining an access password from an ADP system user (whose identity has already been authenticated, perhaps using a personal password); (2) comparing the access password with the password associated with the protected data; and (3) authorizing access to the data if the entered password and the stored password are the same [see note under AUTHENTICATION PROCESS]. (FIPS PUB 112)
automated data processing security	See COMPUTER SECURITY.
automated decision-making computer	***Computer applications that issue checks, requisition supplies, or perform similar functions based on programmed criteria, with little human intervention. (AFR 205-16)***
automated information systems(s) (AIS)	1) An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data and information. (DODD 5200.28) 2) Automated information systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment. (NSDD-145; NTISSP 200) 3) An information system (as defined in Section 6d of the Circular) that is automated. (A-130)

automated information systems security	*1) Measures and controls that protect an AIS against denial of service and unauthorized, (accidental or intentional) disclosure, modification or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS. (NCSC-TG-004-88)* 2) See COMPUTER SECURITY.
automated security monitoring	1) The use of automated procedures to ensure that automation security controls are not circumvented. (AR 380-380) 2) The use of automated procedures to ensure that the security controls implemented within an ADP system are not circumvented. (FIPS PUB 39)
automatic data processing (ADP) system	An assembly of computer hardware, firmware, and software, configured for the purpose of calculating, computing, sorting, transmitting, receiving, storing and retrieving data with a minimum of human intervention. (CSC-STD-005-85; DOD 5200.28-STD; DOE 5635.1A)

automation security

1) The measures employed to protect automation and the information handled from both hostile and benign threats and to safeguard against unauthorized exploitation through espionage, sabotage, theft, fraud, misappropriation, or misuse. Automation security applies to all ADP systems and applies to the global aspects of the security problem. Therefore, it encompasses the security management, hardware, software, procedural, communications, personnel, physical and environmental, and all other security aspects contributing to the protection of automated systems (hardware and software), site, activity, facility, or operation as a potential target. (AR 380-380)

2) See COMPUTER SECURITY.

availability

The computer security characteristic that makes sure the computer resources are available to authorized users when they need them. This characteristic protects against denial of service. (AFR 205-16)

- B -

backdoor	See TRAP DOOR.
backup plan	See CONTINGENCY PLANS.
backup procedures	The provisions made for the recovery of data files and program libraries, and for restart or replacement of ADP equipment after a system failure or disaster. (AR 380-380; FIPS PUB 39)
bandwidth	A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second. (DOD 5200.28-STD)
basic software (nonfunctional)	***Routines and programs designed to extend or facilitate the use of particular automated equipment. As a rule, the vendor provides basic software. It is usually essential for the system operation. Examples of basic software are executive and operating systems, diagnostic programs, compilers, assemblers, utility routines (such as sort-merge and input or output conversion routines), file management programs, and data management programs. (AFR 205-16)***
Bell-LaPadula Model	A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined, and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving that the system is secure. A system state is defined as "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. See *-PROPERTY and ***SIMPLE SECURITY PROPERTY.*** (DOD 5200.28-STD)

benign environment

A nonhostile envelope protected from external hostile elements by physical, personnel, and procedural security countermeasures. In this environment, the ADP system is protected at the system's highest level. All users are cleared for the highest level but a need-to-know is not required for all data. Reliance is placed on the ADP system for routing and need-to-know separation of data. (AR 380-380)

between-the-lines entry

1) Access obtained through active wiretapping by an unauthorized user to a momentarily inactive terminal of a legitimate user assigned to a communications channel. (AR 380-380; FIPS PUB 39)

2) Unauthorized access obtained by tapping the temporarily inactive terminal of a legitimate use. See PIGGYBACK. (NCSC-TG-004-88)

beyond A1

A level of trust defined by the DOD TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC) that is beyond the state-of-the-art technology available at the time the criteria was developed. It includes all the A1-level features plus additional ones not required at the A1 level. (NCSC-TG-004-88)

biometric

The use of specific quantities that reflect unique personal characteristics (such as a fingerprint, an eye blood vessel print, or a voice print) to validate the identity of users. (WB)

BLACK

Refers to unclassified information or equipment and wire lines that handle encrypted classified information. (AFR 205-16)

BLACK equipment area (BEA)

A BLACK equipment area is located in a limited exclusion area. (NACSIM 5203)

bounds checking

1) Testing of computer program results for access to storage outside authorized limits. (AR 380-380; FIPS PUB 39)

2) Synonymous with MEMORY BOUNDS CHECKING.

bounds register

A hardware register which holds an address specifying a storage boundary. (FIPS PUB 39; AR 380-380)

breach

The successful and repeatable defeat of security controls with or without an arrest, which if carried to consummation, could result in a penetration of the system. Examples of breaches are:

a. Operation of user code in master mode.

b. Unauthorized acquisition of identification password or file access passwords.

c. Accessing a file without using prescribed operating system mechanisms.

d. Unauthorized access to tape library. (OPNAVINST 5239.1A; AR 380-380; DOD 5200.28M)

brevity code/ brevity list

A code which has the sole purpose of shortening messages rather than the concealment of their content. (NCSC-9)

brevity lists

1) A pseudo code system that is used to reduce the length of time required to transmit information by use of a few characters in place of long routine sentences. (AR 380-380)

2) A code system that is used to reduce the length of time required to transmit information by the use of a few characters to represent long, stereotyped sentences. (FIPS PUB 39)

broadband emanation or emission

1) An acoustic emanation which is characterized by the following: a. The appearance of the observed emanation is definitely not sinusoidal. b. The duration of the impulse emanation is very short compared with the period between impulses. c. The peak value of the impulse emanation is very much greater (in order of 10 to 15 dB) than the average "apparent r.m.s." value of the overall emanation. (NACSEM 5103)

2) Any electromagnetic emanation or ambient signal detected with broadband tunable or broadband nontunable detection system. (NACSEM 5201)

browsing	1) The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (OPNAVINST 5239.1A; AR 380-380; FIPS PUB 39; ***NCSC-TG-004-88***) 2) Browsing is the unauthorized looking through, identifying, and exploiting of data that are available but are supposed to be unknown. (JL)
bugging	Implanting a physical listening or transmitting device on or in AIS hardware to gain unauthorized access to data being processed. (JCS PUB 6-03.7)

- C -

call back

1) A procedure for identifying a terminal dialing into a system by disconnecting the caller and reestablishing the connection by the computer system dialing the telephone number of the calling terminal. (AR 389-380)

2) Procedure where the system (after identifying the caller) disconnects the call, and dials the caller's computer. Used in an attempt to ensure both the identity and location of the caller. (BBD)

3) A procedure for identifying a remote terminal. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to re-establish the connection. (NCSC-TG-004-88)

4) Synonymous with DIAL BACK.

capability

In a computer system, an unforgeable ticket that is accepted by the system as incontestable proof that the presenter has authorized access to the object named by the ticket. It is often interpreted by the operating system and the hardware as an address for the object. Each capability also contains authorization information identifying the nature of the access mode (for example read mode, write mode). (MTR-8201)

category(ies)

1) Restrictive labels that have been applied to classified or unclassified data as a means of increasing the protection of and further restricting access to the data. Examples include SCI, Proprietary Information, Warning Notice - Intelligence Sources and Methods involved, and NATO. Individuals may be given access to this information only if they have been granted formal access authorization. (AFR 205-16)

2) A grouping of classified or unclassified but sensitive information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have appropriate authorization. (CSC-STD-003,-85)

3) A grouping of classified or unclassified but sensitive information, to which an additional restrictive label is applied (e.g., proprietary, compartmented information). (CSC-STD-004-85)

4) A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information). (DODD 5200.28)

5) A grouping of information to which an additional restrictive label is appiied to signify that personnel are granted access to the information only if they have appropriate authorization (e.g., Restricted Data [RD]). (DOE 5637.1)

caution statement

1) A statement affixed to computer outputs which contains the highest classification being processed at the time the product was produced and a requirement that any data not requested be controlled at that level and returned immediately to the originating computer center. (AR 380-380)

2) See SAFEGUARDING STATEMENT.

central computer facility

One or more computers with their peripherals and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links. (DCID 1/16; AR 380-380)

certification

1) A statement that specifies the extent to which the security measures meet specifications. It does not imply a guarantee that the described system is impenetrable. It is an input to the security approval process. (AFR 205-16)

2) A statement based on detailed technical analysis that specifies the extent to which the security measures in the system or facility meet the security requirements. Certification is based on the results of the risk analysis performed. It does not necessarily imply a guarantee that the described system is impenetrable. It is an input to the security accreditation process. (AFR 700-10)

3) The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements. (DOD 5200.28-STD)

4) The technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which establishes the extent to which a particular AIS design and implementation meet a set of specified security requirements. (DODD 5200.28)

5) Formal written assurance that, based on evaluationof security tests, the classified ADP system and its environment meet the security specifications outlined by the approved ADP security plan. (DOE 5637.1)

6) The technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which the design and implementation of a computer system or network meet prespecified security requirements. (FIPS PUB 39; AR 380-380)

7) The technical process evaluation, made as part of and in support of the accreditation process, whereby a procedure, program, system, component, or system is shown to be secure; i.e., that the security design specifications are correct and have been properly implemented. Certification is performed by independent technical personnel according to an acceptable standard of proof such that the level of security protection is identified with regard to a procedure, program, system component, or system. (OPNAVINST 5239.1A)

8) A reasonable assurance (based on a technical evaluation of a system test) and written acknowledgement made by a CPPM, or an individual designated by the CPPM, that a proposed unclassified computer application processing sensitive information meets all applicable federal and departmental policies, regulations, and procedures, and that results of a systems test demonstrate installed security safeguards are adequate and functioning properly. (DOE 1360.2A)

9) The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements. (NCSC-TG-004-88)

channel — An information transfer path within a system. May also refer to the mechanism by which the path is effected. (DOD 5200.28-STD)

cipher system — A cryptosystem in which the cryptographic treatment is applied to plain text elements of equal length. (AR 380-380; FIPS PUB 39; NCSC-9)

cipher text — 1) Unintelligible text or signals produced through the use of cipher systems. (AR 380-380; FIPS PUB 39)

2) Enciphered information. (NCSC-9)

class — ***A hierarchical ranking that denotes a certain level of trust based on DOD Standard 5200.28-STD. (AFR 205-16)***

classification — A determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made. Data classification is used along with categories in the calculation of risk index. (CSC-STD-004-85; DOE 5635.1A)

classified computer security program	All of the technological safeguards and managerial procedures established and applied to ADP facilities and ADP systems (including computer hardware, software, and data) in order to ensure the protection of classified information. (DOE 5637.1)
classification	A determination that information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made. Data classification is used along with categories in the calculation of risk index. (CSC-STD-004-85; DOE 5635.1A)
classified computer security program	All of the technological safeguards and managerial procedures established and applied to ADP facilities and ADP systems (including computer hardware, software, and data) in order to ensure the protection of classified information. (DOE 5637.1)
classified data/ information	1) Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under E.O. 12356, or prior orders, DOD 5200.1-R, to require protection against unauthorized disclosure; and (c) so designated. (DODD 5200.28) 2) Top Secret, Secret, and Confidential information of all categgries (RD, FRD, NSI, etc.), including intelligence information, for which the department is responsible and requires safeguarding in the interest of national security and defense. (DOE 5637.1; DOE 5635.1A) 3) Official data which has been determined to require protection in the interests of national security. (OPNAVINST 5239.1A)
classified defense information	Official information which requires protection against unauthorized disclosures in the interest of the national security and which has been so designated in accordance with the provision of Executive Order 12356: Top Secret, Secret, Confidential. (AR 380-380)

clearing

The overwriting of classified information on magnetic media such that the media may be reused. (This does not lower the classification level of the media.) Note: Volatile memory can be cleared by removing power to the unit for a minimum of one minute. (DOE 5637.1)

closed security environment

An environment in which both of the following conditions hold true:

1. Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic.

2. Configuration control provides sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during operation of system applications. (CSC-STD-003-85; CSC-STD-004-85)

closed shop

A computer operations area set up such that physical access controls restrict programmers, and others who do not have a need to be present, from being in the area. (WB)

code

Any system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. Coding has three distinctly different applications:

a. In the broadest sense, coding is a means of converting information into a form suitable for communications or encryption; e.g., coded speech, Morse code, teletypewriter codes, etc. No security is provided.

b. Brevity lists are codes which are used to reduce the length of time necessary to transmit information; e.g., long, stereotyped sentences may be reduced to a few characters which are transmitted. No security is provided.

c. A cryptosystem in which the cryptographic equivalents (usually called code groups) typically consisting of letters or digits (or both) in otherwise meaningless combinations are substituted for plain text information elements which are primarily words, phrases, or sentences. Security is provided. (NCSC-9)

code group

A group of letters or numbers, or both, assigned in a code system to represent a plaintext element which may be a word, phrase or sentence. (NCSC-9)

code system

1) a. Any system of communication in which groups of symbols are used to represent plain text elements of varying length.

b. In the broadest sense, a means of converting information into a form suitable for communications or encryption, for example, coded speech, Morse Code, teletype-writer codes.

c. A cryptographic system in which cryptographic equivalents (usually called code groups) typically consisting of letters, digits, or both in meaningless combinations are substituted for plain text elements which may be words, phrases, or sentences. (FIPS PUB 39)

See BREVITY LISTS.

coercive force

A negative or reverse magnetic force applied for the purpose of reducing magnetic flux density. (CSC-STD-005-85)

coercivity

The measure of the amount of coercive force required to reduce magnetic flux density to zero. Often used to represent the ease with which magnetic ADP media can be degaussed. (CSC-STD-005-85)

collateral

All national security information classified under the provisions of an Executive Order for which special intelligence community systems of compartmentation (i.e., sensitive compartmented information) are not formally established. (NACSIM 5203)

communications devices

An active or passive device dedicated to carry information among other devices and performs no processing except that necessary to carry the information (e.g., networks, direct line connections). (JCS PUB 6-03.7)

communications security (COMSEC)

1) Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emission security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to communications security information or materials. (AR 380-380; NCSC-9)

2) The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (DOE 5637.1)

3) The protection that insures the authenticity of telecommunications and that results from the application of measures taken to deny unauthorized persons information of value which might be derived from the acquisition of telecommunications. (FIPS PUB 39)

4) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes:

a. Cryptosecurity. The component of communi- cations security which results from the provision of technically sound cryptosystems and their proper use.

b. Transmission security. The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

c. Emission security. The component of communications security which results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto- equipment and telecommunications systems.

d. Physical security. The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JCS PUB 1)

5) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emmission security, and physical security of communications security materials and information. (OPNAVINST 5239.1A; AFR 700-10)

compartment — Used to describe information that has need-to-know access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. (See also "Sensitive Compartment Information" and "Special Access Program"). (JCS PUB 6-03.7)

compartmentalization — The isolation of the operating system, user programs, and data files from one another in main storage in order to provide protection against unauthorized or concurrent access by other users or programs. This term also refers to the division of sensitive data into small, isolated blocks for the purpose of reducing risk to the data. (AR 380-380; FIPS PUB 39)

compartment "S" variable	The variable held only by members of a select community of interest to ensure compartmentation of calls. (NACSI 8108)
compartmented information	Any information for which the responsible office of primary interest (OPI) requires an individual needing access to that information to possess a special authorization. (CSC-STD-004-85)
compartmented intelligence/sensitive compartmented information (SCI)	Includes only that intelligence material having special controls indicating restrictive handling for which systems of compartmentalization of handling are formally established. (DOD 5200.28M; OPNAVINST 5239.1A)
compartmented security mode	***1) The mode of operation which allows the system to process information at a specified maximum classification level but is capable of reliably separating information among different compartments transmitted by the network. In this mode, system users need not be cleared for all types of compartmented information processed, but they must be fully cleared for at least the highest level of classified information. (NCSC-TG-004-88)*** 2) Utilization of a resource-sharing computer system for the concurrent processing and storage of: (1) two or more types of SCI or (2) one type of SCI with other than SCI. For DON purposes, the compartmented mode should be considered equivalent to multilevel mode. (OPNAVINST 5239.1A)
competent authority	***Authority recognized by the DAA as having sufficient knowledge (individually or corporately) to make a valid determination. (AFR 205-16)***
compliance review	Refers to a review and examination of records, procedures, and review activities at a site in order to assess the unclassified computer security posture and ensure compliance with this order. This review is normally conducted by the CPPC at an operations office having cognizance over the site and management responsibilities for implementing this Order. For those sites not reporting to an operations office, this review is normally conducted by the Office of ADP Management. (DOE 1360.2A)

compromise

1) The disclosure of classified data to persons who are not authorized to receive such data. (DOE 5637.1; DOE 5635.1A)

2) An unauthorized disclosure or loss of sensitive information. (FIPS PUB 39)

3) [Passwords] Disclosing a password, or part of a password, to someone not authorized to know, have or use the password. (FIPS PUB 112)

4) The known or suspected exposure of clandestine personnel, installations or other assets, or of classified information or material, to an unauthorized person. (NCSC-9)

5) An unauthorized disclosure or loss of sensitive defense data. (OPNAVINST 5239.1A; AR 380-380)

6) A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred. (NCSC-TG-004-88)

compromising emanations

1) Electromagnetic emanations that may convey data and that, if intercepted and analyzed, may compromise sensitive information being processed by any ADP system. (FIPS PUB 39)

2) Unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information transmitted, received, handled or otherwise processed by any information-processing system. (NCSC-9)

3) Unintentional data related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmission received, handled or otherwise processed by any information processing equipment. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the "compromising emanations." (OPNAVINST 5239.1A; AFR 700-10; AR 380-380; DOE 5637.1)

	4) Unintentional, data-related, intelligence bearing signals which, if intercepted and analyzed, could disclose the classified information ransmitted, recieved, handled, or otherwise tprocessed by electronic equipment. (AFR 205-16)
computer	A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices. (DODD 5200.28)
computer abuse	***1) Willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation. Levels of computer abuse are:*** ***a. Minor Abuse - Acts that represent management problems (printing calendars or running games), but do not impact system availability for authorized applications;*** ***b. Major Abuse - Unauthorized use (possibly criminal), resulting in denial of service, multiple instances of minor abuse, or waste;*** ***c. Criminal Act - Fraud, embezzlement, theft, malicious damage, misappropriation, conflict of interest, and unauthorized access to classified data. (AFR 205-16)*** ***2) The misuse, alteration, disruption or destruction of data processing resources. The key aspect is that it is intentional and improper. (NCSC-TG-004-88)***
computer crime	Fraud, embezzlement, unauthorized access, and other "white collar" crimes committed with the aid of or directly involving a computer system and/or network. (GAO)
computer cryptography	The use of a crypto-algorithm in a computer, microprocessor or microcomputer to perform encryption/decryption to protect information or to authenticate users, sources, or information. (NCSC-9)

computer facility	***Physical resources that include structures or parts of structures to house and support capabilities. For small computers, stand-alone systems, and word processing equipment, it is the physical area where the computer is used. (AFR 205-16)***
computer fraud	***Computer-related crimes involving deliberate misrepresentation, alteration or disclosure of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or coverup of the act or series of acts. A computer system might have been involved through improper manipulation of input data; output or results; applications programs; data files; computer operations; communications; or computer hardware, systems software or firmware. (NCSC-TG-004-88)***
computer installation	The physical space which contains one or more computer systems. Computer installations may range from locations for large centralized computer centers to locations for individual stand-alone micorcomputers. (DOE 1360.2A)
computer network	1) A complex consisting of two or more interconnected computers. (AR 380-380) 2) See NETWORK.
computer protection plan	A document which serves as the single source management summary of information associated with the DOE unclassified computer security program as required on page 8, under paragraph 11d. It serves as a basis for estimating security needs, performing security assessments, performing compliance and management reviews, and facilitating risk management and certification efforts. (DOE 1369.2A)
computer security (COMPUSEC)	1) The protection of the information and physical assets of a computer system. The protection of information aims to prevent the unauthorized disclosure, manipulation, destruction or alteration of data. The protection of physical assets implies security measures against theft, destruction or misuse of equipment, i.e., processors, peripherals, data storage media, communication lines and interfaces. (MS)

2) The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system. (NCSC-9)

3) All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive unclassified or critical data, material, or processes in the system. It includes:

a. Hardware and software functions, characteristics, and features.

b. Operational procedures.

c. Accountability procedures.

d. Access controls at computer facilities (includes those housing mainframes, terminals, minicomputers, or microcomputers).

e. Management constraints.

f. Physical protection.

g. Control of compromising emanations (TEMPEST).

h. Communications security (COMSEC).

i. Personnel security.

j. Other security disciplines. (AFR 205-16)

4) See ADP SECURITY, ADP SYSTEM SECURITY, AUTOMATED DATA PROCESSING SECURITY, AUTOMATED INFORMATION SYSTEMS SECURITY, AUTOMATION SECURITY, CLASSIFIED COMPUTER SECURITY PROGRAM, DATA SECURITY, INFORMATION SECURITY, INFORMATION SYSTEM SECURITY, and OPERATIONAL DATA SECURITY.

computer security incident	1) An adverse event associated with an ADP system(s): a. that is a failure to comply with security regulations or directives; b. that results in attempted, suspected or actual compromise of classified information; or c. that results in the waste, fraud, abuse, loss or damage of government property or information. (DOE 5637.1) 2) The occurrence of an event which has or could adversely affect normal computer operations such as an unauthorized access, interruption to computer service or safeguarding controls, or discovery of a vulnerability. (DOE 1360.2A) 3) See SIGNIFICANT COMPUTER SECURITY INCIDENT.
computer security subsystem	***A device designed to provide limited computer security features in a larger sysem environment. (NCSC-TG-004-88)***
computer security technical vulnerability reporting program (CSTVRP)	***A program that focuses on technical vulnerabilities in commercially available hardware, firmware and software products acquired by DOD. CSTVRP provides for the reporting, cataloging, and discreet dissemination of technical vulnerability and corrective measures information to DOD components on a need-to-know basis. (NCSC-TG-004-88)***
computer site	A geographic location where one or more computer installations is managed and operated. (DOE 1360.2A)

computer system	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and includes computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949. (PL 100-235)
COMSEC crypto-algorithm	Well-defined procedure or sequence of rules or steps which are used to produce cipher-text from piain-text or vice versa. (NTISSI 4002)
concealment system	A method of achieving confidentiality in which sensitive information is hidden by embedding it in irrelevant data. (FIPS PUB 39; AR 380-380)
conducted signals	Electromagnetic or acoustic emissions of undesired signal data which become induced and propogated along wirelines or other conductors. (NACSEM 5106)
confidentiality	***1) The computer security characteristic that makes sure individuals are given access to computer resources based on security clearance and need-to-know. This characteristic protects against compromise and inadvertent disclosure. (AFR 205-16)*** 2) A concept that applies to data that must be held in confidence and that describes the status and degree of protection that must be provided for individuals or organizations. (AR 380-380; FIPS PUB 39) ***3) The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. (NCSC-TG-004-88)***
configuration control	***The process of controlling modification to the system's hardware, firmware, software and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during and after system implementation. (NCSC-TG-004-88)***

configuration management	***1) Process of controlling modifications to the system hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation. (AFR 205-16)***
	2) The management of security features and assurances through control of changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system. (NCSC-TG-004-88)
	3) The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of insuring that such changes will not lead to decreased data security. (OPNAVINST 5239.1A)
confinement	1) Allowing a process executing a borrowed program (in general, an arbitrary program) to have access to data, while ensuring that the data cannot be misused, altered, destroyed or released. (MTR-8201)
	2) The prevention of the leaking of sensitive data from a program. (NCSC-TG-004-88)
confinement channel	See COVERT CHANNEL.
confinement property	See STAR PROPERTY (*-PROPERTY).
contained	"Contained" refers to a state of being within limits, as within system bounds, regardless of purpose or functions, and includes any state of storage, use, or processing. (OPNAVINST 5239.1A; AR 380-380; DOD 5200.28M)
container	A repository of data in a system. (MTR-8201)
contamination	***1) The introduction of data of one sensitivity and need-to-know with data of a lower sensitivity or different need-to-know. This can result in the contaminating data not receiving the required level of protection. (AFR 205-16)***

2) The intermixing of data at different sensitivity and need-to-know levels. The lower level data is said to be contaminated by the higher level data; thus, the contaminating (higher level) data may not receive the required level of protection. (NCSC-TG-004-88)

contents

When used with respect to a communication, it includes any information concerning the identity of the parties thereto or the existence or meaning of that communication. (NACSI 4000A)

contingency management

Management of all the actions to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical ADP systems and which will facilitate maintaining the continuity of operations in an emergency situation. (DOE 5637.1)

contingency plan(s)

1) A plan for emergency response, backup operations, and post-disaster recovery maintained by an ADP activity as a part of its security program. A comprehensive, consistent statement of all the actions (plans) to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical ADP resources and which will facilitate maintaining the continuity of operations in an emergency situation. (OPNAVINST 5239.1A)

2) Documents, developed in conjunction with computer application owners and maintained at the primary and backup computer installation; they describe procedures and identify personnel necessary to respond to abnormal situations, and ensure that computer application owners can continue to process mission-essential applications in the event that computer support is interrupted (e.g., appropriate automated and/or manual backup processing capabilities). (DOE 1360.2A)

3) A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Also called disaster plan and emergency plan. (NCSC-TG-004-88)

continuity of operations	The maintenance of essential services for an information system after a major failure at an information center. The failure may result from natural causes (such as fire, flood or earthquakes) or from deliberate events (such as sabotage). (GAO)
controllable isolation	Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set or sphere of activity. (FIPS PUB 39; AR 380-380)
controlled access	Synonymous with ACCESS CONTROL.
controlled access area (CAA)	***1) Part or all of an environment where all types and aspects of an access are checked and controlled. (AFR 205-16)*** 2) The complete building or facility area under direct physical control which can include one or more limited exclusion areas, controlled BLACK equipment areas, or any combination thereof. (NACSIM 5203)
controlled accessibility	Synonymous with ACCESS CONTROL.
controlled access protection	Is the C2 level of protection described in the Trusted Computer System Evaluation Criteria.The major characteristics of controlled access protection are addressed in Section IV. (NTISSP 200)
controlled area	***1) Any area, building, or structure specifically designated by the installation commander requiring limited entry for the protection of Air Force personnel or resources. (AFR 205-16)*** 2) An area or space to which access is physically controlled. (NCSC-9) 3) An area within which uncontrolled movement does not permit access to classified information and which is designed for the principal purpose of providing administrative control, safety, or a buffer area of security restrictions for limited exclusion areas. This area may be protected by physical security measures, such as sentries and fences. (OPNAVINST 5239.1A)

controlled BLACK equipment area(s) (CBEA)

A BLACK equipment area which is not located in limited exclusion area but is afforded the same physical entry control which would be required if it were within a limited exclusion area. (NACSIM 5203)

controlled cryptographic item (CCI)

A secure telecommunications or information handling equipment, or associated cryptographic component, which is unclassified but controlled. Equipments and components so designated shall bear the designator "controlled cryptographic item" or "CCI". Replaces the term "Controlled COMSEC Item (CCI) as defined in NCSC-9. (NTISSI 4001)

controlled security mode

1) A mode of operation where internal security controls prevent inadvertent disclosure. Personnel, physical, and administrative controls prevent attempts to gain unauthorized access. The system may have users with access to the system who have neither the security clearance nor need-to-know for all classified information in the system. Access must be limited to users with a minimal security clearance of one less than the highest classified information processed. (AFR 205-16)

2) An automated system is operating in the controlled security mode when at least some users with access to the system have neither the required security clearance nor a need-to-know for all classified material contained in the system. However, the separation and control of users and classified material are not accomplished by the operating system as in the Miltilevel Security Mode. Instead, it is accomplished by the implementation of security measures which reduce or eliminate most system software vulnerabilities. (AR 380-380)

4) An ADP system is operating in the controlled security mode when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material then contained in the ADP system. However, the separation and control of users and classified material on the basis, respectively, of security clearance and security classification is not essentially under operating system control as in the multilevel security mode. (OPNAVINST 5239.1A)

controlled sharing	The condition that exists when access control is applied to all users and components of a resource-sharing system. (AR 380-380; FIPS PUB 39)
controlled space	The three-dimensional space surrounding equipment that processes national security information within which unauthorized personnel are 1) denied unrestricted access and 2) enter escorted by authorized personnel or under continual physical or electronic surveillance. (AFR 700-10)
control zone	1) The space, expressed in feet of radius, surrounding equipment processing classified information which is under sufficient physical and technical control to preclude a successful hostile intercept attack. (AR 380-380) ***2) The space, expressed in feet of radius, surrounding equipment processing sensitive information, that is under sufficient physical and technical control to preclude an unauthorized entry or compromise. (NCSC-TG-004-88)***
copy protected	1) Software distributed on diskettes rendered "uncopyable" by physical means. (BBD) 2) See UNPROTECT.
correctness	1) In a strict sense, the property of a system that is guaranteed as a result of formal verification activities. Correctness is not an absolute property of a system, rather it implies the mutual consistency of a specification and its implementation. (MTR-8201) 2) See VERIFICATION.
correctness proof	A mathematical proof of consistency between a specification and its implementation. It may apply at the security model-to-formal specification level, at the formal specification-to-HOL code level, at the compiler level or at the hardware level. For example, if a system has a verified design and implementation, then its overall correctness rests with the correctness of the compiler and hardware. Once a system is proved correct, it can be expected to perform as specified, but not necessarily as anticipated if the specifications are incomplete or inappropriate. (MTR-8201)

cost-risk analysis

1) The assessment of the costs of potential risk of loss or compromise without data protection versus the cost of providing data protection. (FIPS PUB 39; AR 380-380)

2) The assessment of the costs of providing data protection for a system versus the cost of losing or compromising th edata. (NCSC-TG-004-88)

cots software

Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project. (JCS PUB 6-03.7)

countermeasure

1) That form of military science which by the use of devices and techniques has as its objective the impairment of the operational effectiveness of enemy activity. (AR 380-380)

2) A security feature or control (e.g., hardware, software, personnel, physical, communications or administrative) designed to reduce or eliminate security threats to the ADP system. (JCS PUB 6-03.7)

3) Any action, device, procedure, technique, or other measure that reduces the vulnerability of an ADP system or activity to the realization of a threat. (OPNAVINST 5239.1A)

4) Any action, device, procedure, technique or other measure that reduces the vulnerability of or threat to a system. (NCSC-TG-004-88)

covert channel

1) A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also COVERT STORAGE CHANNEL, COVERT TIMING CHANNEL. (DOD 5200.28-STD; ***NCSC-TG-004-88***)

2) A communication path that allows the transfer of information in a manner which violates system security policy. (AFR 205-16)

covert storage channel	1) A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels. (DOD 5200.28-STD) ***2) A covert channel which involves writing information to a storage location by one process and reading that storage location by a different process. (AFR 205-16)***
covert timing channel	1) A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process. (DOD 5200.28-STD) ***2) A covert channel in which one process modulates its use of system resources (CPU time) to manipulate the real response time observed by a second process thereby signaling information to the second process. (AFR 205-16)***
criteria	See DOD TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA.
critical processing	***Processing which is expected to continue in a correct and uninterrupted manner to support DOD emergency or war plans, preserve human life or safety, or support the mission of the using organization. (AFR 205-16)***
critical resources	Those physical and information assets required for the performance of the site mission. (DOE 5637.1)
criticality	***A measure of how important the correct and uninterrupted functioning of the system is to national security, human life or safety, or the mission of the using organization; the degree to which the system performs critical processing. (AFR 205-16)***

critical technology	Technologies that consist of (a) arrays of design and manufacturing know-how (including technical data); (b) keystone manufacturing, inspection, and test eguipment; (c) keystone materials; and (d) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combinatign of countries and that may prove detrimental to the security of the United States. (Also referred to as military critical technology). (DODD 2040.2; DODD 5230.24; DODD 5230.25)
cross-talk	1) An unwanted transfer of energy from one communications channel to another channel. (FIPS PUB 39; AR 380-380) 2) Undesired energy appearing in one signal path as a result of coupling from other signal paths. Path implies wires, waveguides, or other localized transmission systems. (NACSIM 5203)
crypto	A marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying classified national security information and sensitive, but unclassified government or government-derived information, the loss of which could adversely affect the national security interest. (NTISSI 4002; NACSI 8104)
crypto-algorithm	***A well-defined procedure or sequence of rules or steps used to produce a key stream or cipher text from plain text and vice versa. (NCSC-TG-004-88)***
cryptoanalysis	The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption algorithm. (FIPS PUB 39; AR 380-380)
cryptographic authentication	The use of encryption related techniques to provide authentication. (WB)
cryptographic component	The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or information handling equipment. A cryptographic component may be a modular assembly, a printed circuit board, a microcircuit, or a combination of these items. (NTISSI 4001)

cryptographic equipment	Any equipment employing cryptotechniques or containing cryptographic circuitry or logic. (NACSEM 5201)
cryptographic key	A parameter (e.g., a secret 64-bit number for DES) used by a cryptographic process that makes the process completely defined and usable only by those having that key. (FIPS PUB 112)
cryptographic system	The documents, devices, equipment, and associated techniques that are used as a unit to provide a means of encryption (enciphering or encoding). (FIPS PUB 39; AR 380-380)
cryptography	1) The art or science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form. (FIPS PUB 39; AR 380-380) 2) a. The protection of telecommunications by rendering information unintelligible or unrecognizable until it reaches the intended recipient. b. The design and use of cryptosystems. (NCSC-9) ***3) The principles, means and methods for rendering information unintelligible and for restoring encrypted information to intelligible form. (NCSC-TG-004-88)***
cryptology	1) The field that encompasses both cryptography and cryptoanalysis. (FIPS PUB 39; AR 380-380) 2) The science which deals with hidden, disguised, or encrypted communications. It embraces communications security and communication intelligence. (NCSC-9)
crypto-operation	The functional application of cryptographic methods. a. Off-line. Encryption or decryption performed as a self-contained operation distinct from the transmission of the encrypted text, as by hand or by machines not electrically connected to a signal line.

b. On-line. The use of crypto-equipment that is directly connected to a signal line, making continuous processes of encryption and transmission or reception and decryption. (AR 380-380)

custodian of data

The individual or group that has been entrusted with the possession of, and responsibility for, the security of specified data. (WB)

customer

1) A person or organization who receives products that an automated system produces, but who does not have access to the system. Input and output must be reviewed by cleared knowledgeable people. (AFR 205-16)

2) A civil or military department or agency of the government which uses keying material, classified or unclassified. (NACSI 2002A)

3) See ACCESS.

cycle (for overwriting memory, disk, etc.)

One overwrite cycle is defined as follows: write one bit pattern or character, then write the complement of that pattern or character into every addressable location or sector. (CSC-STD-005-85)

- D -

data	1) Information with a specific physical representation. (DOD 5200.28-STD) 2) A representation of facts, concepts, information, or instructions suitable for for communication, interpretation, or processing by humans or by an AIS. (DODD 5200.28) 3) Information with a specific representation (loosely used to denote any or all information that can be processed, stored or produced by a computer). (CSC-STD-005-85) 4) Programs, files or other information stored in, or processed by, a computer system. (FIPS PUB 112)
database	An extensive and comprehensive set of records collected and organized in a meaningful manner to serve a particular purpose. (DODD 3200.12)
data contamination	1) A deliberate or accidental process or act that results in a change in the integrity of the original data. (AR 380-380; FIPS PUB 39) 2) See DATA DIDDLING.
data-dependent protection	Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements. (FIPS PUB 39; AR 380-380)
data diddling	1) [...]the entering of false data into a computer system. (TC) 2) See DATA CONTAMINATION.
data encrypting key	A cryptographic key used for encrypting (and decrypting) data. (FIPS PUB 112)
data encryption standard (DES)	1) An unclassified crypto-algorithm published by the National Bureau of Standards in FIPS PUB 46 for the protection of certain U.S. Government information. (NCSC-9)

2) A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use. (NCSC-TG-004-88)

data flow control — See INFORMATION FLOW CONTROL.

data integrity — 1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. (AR 380-380; FIPS PUB 39)

2) The state that exists when data is unchanged from its source and accidently or maliciously has not been modified, altered, or destroyed. (DODD 5200.28)

3) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, disclosure, or destruction. (OPNAVINST 5239.1A; AR 380-380; DOD 5200.28-STD)

4) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or willful alteration or destruction. (AFR 205-16)

5) The property that data meets an priori expectation of quality. (NCSC-TG-004-88)

data level

a. Level I. Classified data.

b. Level II. Unclassified data requiring special protection; for example Privacy Act, For Official Use Only, technical documents restricted to limited distribution.

c. Level III. All other unclassified data. (OPNAVINST 5239.1A)

data owner — The authority, individual, or organization who has original responsibility for the data by statute, executive order, or directive. (DODD 5200.28)

data protection engineering	The methodology and tools used for designing and implementing data protection mechanisms. (FIPS PUB 39)
data security	1) The protection of data from accidental or malicious modification, destruction, or disclosure. (FIPS PUB 39) 2) The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (OPNAVINST 5239.1A; AR 380-380)
DC erasure	***Degaussing with a hand-held permanent magnet or with DC electrical-powered equipment to saturate the media so the noise level is raised to mask the signal level. There should be no signal level detectable above the noise level after DC erasure. (AFR 205-16)***
decipher	1) To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into plain text. (AR 380-380) 2) To convert, by use of the appropriate key,enciphered (encoded or enciphered) text into plain text. (FIPS PUB 39) 3) To convert enciphered text into its equivalent plain text by means of cipher system. (This does not include solution by cryptanalysis.) (NACSEM 5201; NCSC-9)
declassification (of magnetic storage media)	***An administrative action following purging of the AIS or magnetic storage media that is the audited step that the owner of the AIS or medium takes when the classification is lowered to UNCLASSIFIED. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities. (NCSC-TG-004-88)***
decode	1) To convert encoded text into its equivalent plain text by means of code. (NCSC-9) 2) Synonymous with DECRYPT.
decrypt	1) To convert, by use of the appropriate key, encrypted (encoded or enciphered) text into its equivalent plain text. (FIPS PUB 39; AR 380-380)

2) To convert encoded text into its equivalent plain text by means of code. (NCSC-9)

3) Synonymous with DECODE.

dedicated security mode

1) The mode of operation in which all users have the appropriate clearance and need-to-know for all data in the system. The system is exclusively dedicated to and controlled for that processing, full-time or for a specified period of time. (AFR 205-16)

2) A mode of operation in effect when all users with access have both a clearance and need-to-know for all information in the information system. Processing may be in this mode full time or for specific periods of time. (AFR 700-10)

3) The mode of operation in which the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (CSC-STD-003-85)

4) A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. (DODD 5200.28)

5) An ADP system is operating in a dedicated mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specified users or groups of users for the processing of a particular type(s) and category(ies) of classified information. (DOD 5200.28M)

6) The operation of an ADP system such that the central computer facility, the connected peripheral devices, the communications facilities, and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information. (FIPS PUB 39)

7) An ADP system is operating in the dedicated security mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or group of users having a security clearance and need-to-know for the processing of a particular category(ies) and type(s) of classified material. (OPNAVINST 5239.1A; AR 380-380)

default classification

A temporary classification, reflecting the highest classification being processed in an automated system. The default classification is included in the safeguard statement affixed to the product. (AR 380-380)

degauss

1) To reduce magnetic flux density to zero by applying a reverse (coercive) magnetizing force. Commonly referred to as demagnetizing. (CSC-STD-005-85)

2) To apply a variable, alternating current (AC) field for the purpose of demagnetizing magnetic recording media. The process involved increases the AC field gradually from zero to some maximum value and back to zero, which leaves a very low residue of magnetic induction on the media. (OPNAVINST 5239.1A; AR 380-380; FIPS PUB 39)

3) To demagnetize, thereby removing magnetic memory. (JCS PUB 6-03.7)

4) To reduce magnetic flux density to zero by applying a reverse magnetizing field. Also referred to as demagnetizing. (NCSC-TG-004-88)

degausser

1) An electrical device (AC or DC) or a hand-held magnet assembly which can generate coercive magnetic force for the purpose of degaussing magnetic storage media or other magnetic material. (CSC-STD-005-85)

2) An electrical devide thatn can generate a magnetic field for the purpose of degaussing magnetic storage media. (NCSC-TG-004-88)

degree of trust

The level of confidence in security mechanisms and procedures to correctly enforce the security policy. (AFR 205-16)

denial of service

1) Action or actions that result in the inability of an AIS or any essential part of an AIS to perform its designated mission, either by loss or degradation of operational capability. (DODD 5200.28)

2) Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Also called interdiction. (NCSC-TG-004-88)

3) See INTERDICTION.

descriptive top-level specification (DTLS)

A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two. (DOD 5200.28-STD)

designated approving authority (DAA)

1) An official who approves the operation of automated systems at the computer facilities under their jurisdiction for processing of information or for critical processing. (AFR 205-16)

2) The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS. (DODD 5200.28)

3) An official assigned responsibility to accredit ADP elements, activities, and networks under the official's jurisdiction. (OPNAVINST 5239.1A)

4) The official who has the authority to decide on accepting the security safeguards prescirbed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. (NCSC-TG-004-88)

designated development activity (DDA)

The activity assigned responsibility by the Joint Chiefs of Staff for development of a standard software capability. (JCS PUB 19)

design verification	The use of verification techniques, usually computer-assisted, to demonstrate a mathematical correspondence between an abstract (security) model and a formal system specification. (MTR-8201)
destruction	The physical alteration of ADP system media or of ADP system components such that they can no longer be used for storage or retrieval of information. (DOE 5637.1)
detection	The act of determining the presence of TEMPEST emanations by technical surveillance techniques. (NACSEM 5106)
detection system	The total instrumentation used in performing an acoustic TEMPEST test which includes the transducer, detector, and display devices. Recording devices are also included if they are the only means of displaying the emanations during the test. (NACSEM 5103; NACSEM 5106; NACSEM 5201)
dial back	See CALL BACK.
dial-up	***The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer. (NCSC-TG-004-88)***
disaster recovery plans	1) Documents containing procedures for emergency response, extended backup operations, and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objectives of these plans, in conjunction with continqency plans, are to provide reasonable assurance that a computer installation can recover from such incidents, continue to process mission-essential applications in a degraded mode (i.e., as a minimum, process computer applications previously identified as most essential), and return to a normal mode of operation within a reasonable amount of time. Such plans are a protective measure generally applied based on assessments of risk, cost, benefit, and feasibility as well as the other protective measures in place. (DOE 1360.2A) 2) See CONTINGENCY PLAN(S).

discretionary access control (DAC)

1) A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (DOD 5200.28-STD; CSC-STD-004-85)

2) A means of restricting access to objects based on the identity and need-to-know of the user, process, and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare MANDATORY ACCESS CONTROL. (NCSC-TG-004-88)

discretionary protection

Access control that identifies individual users and their need-to-know and limits users to the information that they are allowed to see. It is used on systems that process information with the same level of sensitivity. (AFR 205-16)

dissemination of information

The function of distributing government information to the public, whether through printed documents, or electronic or other media. Does not include intra-agency use of information, interagency sharing of information, or responding to requests for "access to information." (A-130)

distribution statement

A statement used in marking a technical document to denote the extent of its availability for distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking assigned in accordance with DOD 5200.1-R. (DODD 5230.24)

distribution system

The metallic wirepaths or fiber optic transmission paths providing interconnection between components of the protected system. (NACSIM 5203)

document	1) Any recorded information regardless of its medium, physical form, or characteristics. a. Technical document. Any document that presents STI. b. Technical report. Any preliminary or final technical document prepared to record, document, or share results obtained from, or recommendations made on, or relating to, DOD-sponsored or co-sponsored scientific and technical work. (DODD 5200.12) 2) Any record of information regardless of physical form or characteristics, including, but not limited to, the following: a. Handwritten, printed, or typed matter. b. Painted, drawn, or engraved matter. c. Sound, magnetic, optical or electro-mechanical recordings. d. Photographic prints and exposed or developed film or still or motion pictures. e. Automatic data processing input and contents of equipment and/or media including memory, punch cards, tapes, diskettes, and visual displays. f. Reproductions of the foregoing by any process. (DOE 5635.1A)
DoD information analysis center (IAC)	An activity that acquires, digests, analyzes, evaluates, synthesizes, stores, publishes, and provides advisory and other user services concerning available worldwide scientific and technical information and engineering data in a clearly defined, specialized field or subject area of significant DOD interest or concern. IACs are distinguished from technical information centers and libraries whose functions are primariiy concerned with providing reference or access to the documents themselves rather that the STI information contained in the documents. (DODD 3200.12)

"DoD Trusted Computer System Evaluation Criteria (TCSEC)	A document published by the NCSC containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is DOD 5200.28-STD and is frequently referred to as "The Criteria" or "The Orange Book." (NCSC-TG-004-88)
domain	The set of objects that a subject has the ability to access. (DOD 5200.28-STD)
dominate	Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all of those of S2 as a subset. (DOD 5200.28-STD)
dual control	The process of utilizing two or more separate entities (usually persons) operating in concert, to protect sensitive functions or information. Both (all) entities are equally responsible. This approach generally involves the split-knowledge [of the] physical or logical protection of security parameters. (WB)
dumb terminal	Terminal (or computer using dumb terminal software) which allows communications with other computers, but does not enhance the data exchanged, or provide additional features such as upload/download. (BBD)

- E -

eavesdropping	The unauthorized interception of information-bearing emanations through the use of methods other than wiretapping. (FIPS PUB 39; AR 380-380)
economic assessment	A detailed study of security measures, their operational and technical feasibility, and their costs and benefits. Economic assessment aids in planning and selecting security measures. (***AFR 205-16***; AFR 700-10)
electromagnetic emanations	Signals transmitted as radiation through the air and through conductors. (FIPS PUB 39; AR 380-380)
electronic funds transfer (EFT)	Electronic funds transfer refers to the movement of value (money) from one party to another by electronic means. (GAO)
electronic surveillance	The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, but not including the use of radio direction-finding equipment soley to determine the location of a transmitter. (NACSI 4000A)
emanations	See COMPROMISING EMANATIONS and ELECTROMAGNETIC EMANATIONS.
emanation security	The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations. (FIPS PUB 39)
embedded system	1) An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e.g., ground support equipment, flight simulators, engine test stands, or fire control systems. (DODD 5200.28) ***2) Computers which are dedicated elements, subsystems, or components of more extensive Air Force systems. (AFR 205-16)***
emergency plan	See CONTINGENCY PLAN(S).

emission security

1) A component of COMSEC that results from all measures to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from electrically operated classified information processing equipment and systems. (AR 380-380)

2) That component of communications security (COMSEC) which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. (NCSC-9; JCS PUB 1)

3) The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems. (NCSC-TG-004-88)

emulator

A combination of hardware and software that permits programs written for one computer to be run on another computer. In computer security terminology, the emulator is the portion of the system responsible for creating an operating system compatible environment out of the environment provided by the kernel. (MTR-8201)

encipher

1) To convert plain text into an unintelligible form by means of a cipher system. (FIPS PUB 39; AR 380-380)

2) To convert plain text into enciphered text by means of a cipher system. (NCSC-9)

encode

1) To convert plain text into an unintelligible form by means of a code system. (FIPS PUB 39; AR 380-380)

2) To convert plain text into encoded text by means of a code system. (NCSC-9)

encrypt

1) To convert plain text into unintelligible form by means of a cryptosystem. (AFR 700-10; AR 380-380; FIPS PUB 39)

2) To convert plain text into unintelligible form by means of a cryptosystem. Note: The term encrypt encompasses the terms "encipher" and "encode." (NCSC-9)

encryption

1) Transforming a text into code in order to conceal its meaning.

a. End-to-end encryption. Encryption of information at the origin within a communications network and postponing decryption to the final destination point.

b. Link encryption. The application of on-line crypto-operations to a link of a communications system so that all information passing over the link is encrypted. (AR 380-380)

2) The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption). (FIPS PUB 112)

3) See END-TO-END ENCRYPTION and LINK ENCRYPTION.

encryption algorithm

1) A set of mathematical rules for rendering information unintelligible by effectinq a series of transformations to the normal representation of the information through the use of variable elements controlled by a key. (AR 380-380)

2) A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a key to the normal representation of the information. Synonymous with PRIVACY TRANSFORMATION. (FIPS PUB 39)

end-to-end encryption

1) Encryption of information at the origin within a communications network and postponing decryption to the final destination point. (FIPS PUB 39)

	2) The protecton of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination. (NCSC-TG-004-88)
	3) See ENCRYPTION and LINK ENCRYPTION.
entrapment	1) The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations. (AR 380-380)
	2) The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit. (FIPS PUB 39)
entry	See BETWEEN-THE-LINES ENTRY and PIGGY BACK ENTRY.
environment	1) The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. (CSC-STD-004-85; CSC-STD-003-85)
	2) The aggregate of external procedures, conditions, and objects that affect the development, operaiton, and maintenance of a system. (NCSC-TG-004-88)
erasure	1) A security model rule stating that objects must be purged before being activated or reassigned. This ensures that no information is retained within an object when it is reassigned to a subject at a differing security level. (MTR-8201)
	2) A process by which a signal recorded on magnetic media is removed (i.e., degaussed). Erasure may be accomplished in two ways: in AC erasure the media are degaussed by applying an alternating field which is reduced in amplitude from an initial high value (i.e., AC powered); in DC erasure, the media are saturated by applying a unidirectional field (i.e., DC powered or by employing a permanent magnet). (CSC-STD-005-85)

escort(s)

Duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security implications of and to control the activities and access of the individual being escorted. (OPNAVINST 5239.1A; AR 380-380; DCID 1/16; DCID 1/16, Sup.; DOD 5200.28M)

essential elements of friendly information (EEFI)

Key questions about friendly intentions and military capabilities asked by opposing planners and decision makers. This information if acquired by hostile interests by any means, might jeopardize the successful execution of an operation. (AFR 205-16)

essentially rating

An importance-time-related designation assigned to a computer application that indicates when an application must be back in operation to avoid mission impacts after a disaster or interruption in computer support services at a multiuser installation. To facilitate prioritized recovery procedures and for operating at offsite backup facilities in a degraded mode (i.e., only most essential applications), computer applications should be assigned essentiality ratings of varying importance (e.g., most essential, essential, important, defferable). Applications with the same essentiality rating (i.e., most essential) should be additionally ranked (e.g., numerically) according to installation or site determined processing priorities and perceptions of importance. (DOE 1360.2A)

evaluated products list (EPL)

1) A documented inventory of commercially available trusted computer hardware and software that has been evaluated against the Department of Defense Trusted Computer System Evaluation Criteria by the National Computer Security Center. (***AFR 205-16***; DODD 5215.1)

2) A documented inventory of equipments, hardware, software, and/or firmware that has been evaluated against the evaluation criteria found in DOD 5200.28-STD. (DODD 5200.28)

	3) A list of equipments, hardware, software, and/or firmware that have been evaluated against, and found to be technically compliant, at a particular level of trust, with the DoD TCSEC by the NCSC. The EPL is included in the National Security Agency Information Systems Security Products and Services Catalogue, which is available through the Government Printing Office. (NCSC-TG-004-88)
evaluation	The evaluator's report to the designated approving authority describing the investigative and test procedures used in the analysis of the ADP system security features with a description and results of tests used to support or refute specific system weaknesses that would permit the acquisition of identifiable classified material from secure or protected data files. (DOD 5200.28M)
evaluator	Personnel specifically designated to participate in the test team review, analysis, testing, and evaluation of the security features of an automated system. (AR 380-380)
exclusion area	A security area for the protection of classified matter where mere access to the area would result in access to classified matter. See DOE 5632.4 for further information. (DOE 5637.1)
executive state	1) One of two generally possible states in which a ADP system may operate, and in which, only certain privileged instruction may be executed; such privileged instructions may not be executed when the system is operating in the other, the user state. (FIPS PUB 39; AR 380-380) 2) Synonymous with SUPERVISOR STATE.
exhaustive attack	1) [An] exhaustive attack consists of discovering secret data by trying all possibilities and checking for correctness. For a four digit password, one might start with 0000 and move on to 0001, 0002 till 9999. (JL) 2) See SCANNING.

expired password	A password that must be changed by the user before login may be completed. (CSC-STD-002-85)
exploitable channel	1) Any channel that is usable or detectable by subjects external to the trusted computing base. (DOD 5200.28-STD) 2) See COVERT CHANNEL.
exposure	A specific instance of the condition of being unduly exposed to losses resultinq from the occurrence of one or more threat events. (WB)
external protected distribution system	That portion of a protected distribution system extending beyond a controlled access area (CAA). (NACSIM 5203)
external security audit	A security audit conducted by an organization independent of the one being audited. (FIPS PUB 39)

- F -

fail safe	The automatic termination and protection of programs or other processing operations when a hardware or software failure is detected in an ADP system. (FIPS PUB 39; AR 380-380)
fail soft	The selective termination of affected nonessential processing when a hardware or software failure is detected in an automated system. (AR 380-380; FIPS PUB 39)
failure access	An unauthorized and usually inadvertent access to data resulting from a hardware or software failure in the automated system. (AR 380-380; FIPS PUB 39)
failure control	The methodology used to detect and provide fail-safe or fail-soft recovery from hardware and software failures in an automated system. (AR 380-380; FIPS PUB 39)
fault	1) A condition that causes a device or system component to fail to perform in a required manner (such as, a short circuit, broken wire, or intermittent connection). (AR 380-380) 2) Synonym for LOOPHOLE.
features	See SECURITY FEATURES.
federal computer system	A computer system operated by a federal agency or by a contractor of a federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a federal function;, and includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. (PL 100-235)
fetch protection	A system-provided restriction to prevent a program from accessing data in another user's segment of storage. (FIPS PUB 39; AR 380-380)

file authentication code	In a manner similar to that used for the computation of a message authentication code, certain authentication techniques can be used to provide assurance that data held in a file has not been altered or deleted. This term is also applied to databases. (WB)
file protection	The aggregate of all processes and procedures established in an automated system and designed to inhibit unauthorized access, contamination, or elimination of a file. (AR 380-380; FIPS PUB 39)
filter	A device for use on power, signal, telephone or other wirelines, specifically designed to pass only selected frequencies and to attenuate substantially all other frequencies. There are two basic types of filters: 1) active filters - Those which are active components and require the application of power for the utilization of their filtering properties. 2) passive filters - Those which use passive components having properties of inductance, capacitance or resistance and which do not require the application of power for the utilization of their filtering properties. (NACSIM 5203)
firmware	1) Software that is permanently stored in a hardware device which allows reading but not writing or modifying. The most common device for firmware is read only memory (ROM). (***AFR 205-16***; JCS PUB 6-03.7) 2) Computer programs recorded in a permanent or semipermanent physical medium incorporated in the computer equipment. (AR 380-380)
flaw	1) An error of commission, omission, or oversight in a system that may allow protection mechanisms to be bypassed. (DOD 5200.28-STD) 2) Synonymous with LOOPHOLE. 3) See PSEUDO-FLAW.

flaw hypothesis methodology

A system analysis and penetration technique where specifications and documentation for the system are analyzed and then flaws in the system are hypothesized. The list of hypothesized flaws is then prioritized on the basis of the estimated probability that a flaw exists and, assuming a flaw does exist, on the ease of exploiting it, and on the extent of control or compromise it would provide. The prioritized list is used to direct a penetration attack against the system. (DOD 5200.28-STD)

flow control

1) A strategy for protecting the contents of information objects from being transferred to objects at improper security levels. It is more restrictive than access control. (MTR-8201)

2) See INFORMATION FLOW CONTROL.

foreign government information

1) Information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or information produced by the United States pursuant to or as a result of joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence. (EO 12356)

2) Information that is:

a. Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation either expressed or implied, that the information or the source of information, or both be held in confidence.

b. Produced by the United States following or as a result of a joint arrangement with a foreign government or governments or an international organization of governments or any element thereof, requiring that the information or the arrangement or both be held in confidence. Information described in subparagraphs above and in the possession of the DOD is classified information in accordance with DOD 5200.1-R. (DODD 5230.24; DOE 5635.1A)

formal access approval

Documented approval by a data owner to allow access to a particular category of information. (DODD 5200.28)

formal proof

A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and for showing that computer programs satisfy their specifications. (DOD 5200.28-STD)

formal security policy model

1) A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a TCB, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include: state transition models, denotational semantics models, and algebraic specification models. (DOD 5200.28-STD)

2) See BELL-LAPADULA MODEL and SECURITY POLICY MODEL.

formal top-level specification (FTLS)

A top-level specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven. (DOD 5200.28-STD)

formal verification	The process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model (implementation verification) or between the formal specification and its program implementation. (DOD 5200.28-STD)
formerly restricted data (FRD)	Classified information jointly determined by DOE and the Department of Defense (DOD) to be related primarily to the military utilization of atomic weapons, and removed by DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act, as amended, and safeguarded as national security information subject to the restrictions of transmission to other countries and regional defense organizations that apply to Restricted Data. (DOE 5635.1A)
formulary	A technique for permitting the decision to grant or deny access to be determined dynamically at access time, rather than at the time of creation of the access list. (FIPS PUB 39)
for official use only (FOUO) data	Unclassified official information of a sensitive proprietary, or personal nature which must be protected against unauthorized public release as defined in AFR 12-30. (***AFR 205-16***; AR 380-380)
front-end security filter	A process that is invoked to process data according to a specified security policy prior to releasing the data outside the processing environment or upon receiving data from an external source. (DOD 5200.28-STD)
functional testing	The portion of security testing in which the advertised features of a system are tested for correct operation. (DOD 5200.28-STD)

- G -

gateway	An interface between two networks. (JCS PUB 6-03.7)
gauss	A unit measure of the magnetic flux density produced by a magnetizinq force. (CSC-STD-005-85).
general purpose system	A computer system that is designed to aid in solving a wide variety of problems. (DOD 5200.28-STD)
government agency	1) Any executive department, commission, independent establishment, or corporation, wholly or partly owned by the United States of America and which is an instrumentality of the United States, or any board, bureau, division, service, office, authority, administration, or other establishment in the executive branch of the government. (DOE 5635.1A) 2) Synonymous with AGENCY.
government contractor	An individual, corporation, partnership, association, or other entity performing work under a U.S. Government contract, either as a prime contractor, or as a subcontractor. (NTISSI 3005; NACSI 6002)
government contractor telecommunications	Telecommunications between or among departments or agencies and their contractors, and telecommunications of, between, or among government contractors and their subcontractors, of whatever level, which relate to government business or performance of a government contract. (NACSI 6002)
government information	Information created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the federal government. (A-130)
government publication	Informational matter which is published as an individual document at government expense, or as required by law. (A-130)

government telecommunications	Telecommunications of any employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the U.S. government or a government contractor. (See Telecommunications and and Telecommunications System.) (NACSI 4000A)
granularity	The relative fineness or coarseness by which a mechanism can be adjusted. The phrase "the granularity of a single user" means the access control mechanism can be adjusted to include or exclude any single user. (DOD 5200.28-STD)
group userid	A USERID snared by numerous authorized users. Also implies sharing of the associated Top Secret password. (JCS PUB 6-03.7)
guard	***A processor that provides a filter between two disparate systems operating at different security levels or between a user terminal and a data base to filter out data that the user is not authorized to access. (NCSC-TG-004-88)***
Gypsy	A combined formal program specification language and a verifiable high order language, developed at the University of Texas, and designed in conjunction with a complete verification system. (MTR-8201)

- H -

hacker	Originally, a computer enthusiast who spent significant time learning the functions of the computer without benefit of formal training (and often without the technical manuals) by trying combinations of commands at random to determine their effect. Common usage today is from the press, which uses the word to describe people who "break into" computers for various purposes. (BBD)
handled by	The term "handled by" denotes the activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating and controlling. (DODD 5200.28)
handshaking	Passing control characters between two devices, to control the flow of information. (AFR 205-16)
handshaking procedures	1) A dialogue between a user and a computer, a computer and another computer, a program and another program for the purpose of identifying a user and authenticating identity. A sequence of questions and answers is used based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue. (AR 380-380; FIPS PUB 39) 2) Synonymous with PASSWORD DIALOGUE.
hardware security	Computer equipment features or devices used in an ADP system to preclude unauthorized data access. (AR 380-380)
hash total	The use of specific mathematical formulae to produce a quantity that is (often appended to and) used as a check-sum or validation parameter for the data that it protects. (WB)
hidden sections	Menu options, or entire sub-menus, not visible or accessible to a user due to lack of adequate authorization. (BBD)

hierarchical development methodology (HDM)	A formal specification and verification methodology developed at SRI International. HDM is based on a nonprocedural, state- transition specification language, SPECIAL, and provides a security flow analysis tool, MLS, for verifying the multilevel security properties of a user-interface specification. (MTR-8201)
hostile threat environment	***An area that contains known threats and possesses little or no control over the surrounding area, such as experienced by some diplomatic facilities. (AFR 205-16)***
hot-standby	Equipment and other information system components that are electricaliy activated and so configured such that production operations can be quickly and easily switched to such components. (WB)
human interface functions	TCB operations that require human intervention or judgement. Untrusted processes would not be able to invoke them. (MTR-8201)

identification

1) The process that enables recognition of a user described to an ADP system. This is generally by the use of unique machine-readable names. (AR 380-380)

2) The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to an ADP system. (FIPS PUB 39)

identity token

A smart card, a metal key, or some other physical token carried by a systems user that allows user identity validation. (WB)

identity validation

1) The performance or tests, such as the checking of a password, that enables an information system to recognize users or resources as identical to those previously described to the system. (WB)

2) See AUTHENTICATE and AUTHENTICATION.

impersonation

1) An attempt to gain access to a system by posing as an authorized user. (FIPS PUB 39)

2) Synonymous with MASQUERADING and MIMICKING.

implementation verification

The use of verification techniques, usually computer-assisted, to demonstrate a mathematical correspondence between a formal specification and its implementation in program code. (MTR-8201)

inadvertent disclosure

Accidental exposure of sensitive defense information to a person not authorized access. This may result in a compromise or a need-to-know violation. (AR 380-380; JCS PUB 6-03.7)

Ina Jo (formal development methodology)

System Development Corporation's [now part of UNISYS] specification and verification methodology,based on a nonprocedural state-transition specification language, Ina Jo. The Ina Jo methodology incorporated user-supplied invariants to produce a formal demonstration that security properties are met. (MTR-8201)

incident	See COMPUTER SECURITY INCIDENT.
incomplete parameter checking	A system fault that exists when all parameters have not been fully checked for accuracy and consistency by the operating system, thus making the system vulnerable to penetration. (AR 380-380; FIPS PUB 39)
individual accountability	The ability to positively associate the identity of a user with the time, method, and degree of access to a system. (***NCSC-TG-004-88***; AR 380-380)
information	1) Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. (A-130) 2) The terms "data," "information," "material," "documents," and "matter" are considered synonymous and used interchangeably in this order. They refer to all data regardless of its physical form (e.g., data on paper printouts, tapes, disks or disk packs, in memory chips, Random access memory (RAM), in read only memory (ROM), microfilm or microfiche, on communication lines, and on display terminals). (DOE 5637.1) 3) Any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. (EO 12356; DOE 5635.1A) 4) Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium. (DODD 5200.28) 5) The end product of communication. (NACSEM 5100)
information flow analysis	Tracing the flow of specific information types through an information system to determine whether the controls applied to this information are appropriate. (WB)

information flow control	1) See COVERT CHANNEL, SIMPLE SECURITY PROPERTY, STAR PROPERTY (*-PROPERTY). 2) Synonymous with DATA FLOW CONTROL and FLOW CONTROL.
information resources management	The planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology. (A-130)
information security	1) The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute. (DOD 5200.1-R) 2) See COMPUTER SECURITY.
information system	The organized collection, processing, transmission, and dissemination or information in accordance with defined procedures, whether automated or manual. (A-130; DODD 5200.28)
information system abuse	Willful or negligent activity that affects the availability, confidentiality, or integrity of information systems resources. Includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation. (AFR 700-10)
information systems security	1) The protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and information contained within the systems. Such protection is the application of the combination of all security disciplines which will, at a minimum, include COMSEC, TEMPEST, computer security, OPSEC, information security, personnel security, industrial security, resource protection, and physical security. (AFR 700-10) 2) See COMPUTER SECURITY.

information system security officer (ISSO)	The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal. (DODD 5200.28)
information technology	The hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, or others. Automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. (2) and 10 U.S.C. 2315, are excluded. (A-130)
information technology facility	An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. (A-130)
information technology installation	One or more computer or office automation systems including related telecommunications, peripheral and storage units, central processing units, and operating and support system software. Information technology installations may range from information technology facilities such as large centralized computer centers to individual stand-alone microprocessors such as personal computers. (A-130)
integrity	1) A computer security characteristic that ensures computer resources operate correctly and that the data in the data bases are correct. This characteristic protects against deliberate or inadvertent unauthorized manipulations. This characteristic is applicable to hardware, software, firmware, and the data bases used by the system. (AFR 205-16) 2) The quality or state of being unimpaired; soundness. a. The capability of an automated system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

b. Inherent quality of protection that ensures and maintains the security of entities of a computer system under all conditions. (AR 380-380)

3) The assurance, under all conditions, that a system will reflect the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection mechanisms; and the consistency of the data structures and accuracy of the stored data. In a formal security model, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (MTR-8201)

4) Sound, unimpaired or perfect condition. (NCSC-TG-004-88)

5) See DATA INTEGRITY and SYSTEM INTEGRITY.

intelligence

Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations. (AR 380-380; DOD 5200.28M)

intelligence information

Classified information defined as intelligence information by Director of Central Intelligence Directive 1/16. (DOE 5637.1)

intelligent terminal

A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics. (DODD 5200.28)

interactive computing

Use of a computer such that the user is in control and may enter data or make other demands on the system which responds by the immediate processing of user requests and returning appropriate replies to these requests. (FIPS PUB 39)

interdiction	1) The act of impeding or denying the use of system resources to a user. (FIPS PUB 39; AR 380-380) 2) See DENIAL OF SERVICE.
interface	The commmon boundary between independent systems or modules, where communications takes place. (MTR-8201)
interim approval	The temporary authorization granted an information system to process sensitive or critical information in its operational environment based on preliminary results of a comprehensive security evaluation of the information system. (AFR 700-10)
internal controls	The plan of organization and all of the methods and measures adopted within an agency to safeguard its resources, assure the accuracy and reliability of its information, assure adherence to applicable laws, regulations and policies, and promote operational economy and efficiency. (A-123; DDDD 7040.6)
internal control documentation	Written policies, organization charts, procedural write-ups, manuals, memoranda, flow charts, decision tables, completed questionnaires, software, and related written materials used to describe the internal control methods and measures, to communicate responsibilities and authorities for operating such methods and measures, and to serve as a reference for persons reviewing the internal controls and their functioning. (A-123; DODD 7040.6)
internal control review	A detailed examination of internal control to determine whether adequate control measures exist and are implemented to prevent or detect the occurrence of potential risks in a cost effective manner. (A-123; DODD 7040.6)
internal control system	The totality of the methods and measures of internal control. (A-123; DODD 7040.6)
internal protected distribution system	That portion of a protected distribution system located entirely within a controlled access area (CAA). (NACSIM 5203)

internal security audit	A security audit conducted by personnel responsible to the management of the organization being audited. (FIPS PUB 39)
internal security controls	***Hardware, firmware, and software features in an automated system that restrict access to resources (hardware, software, and data) to only authorized persons, programs, or devices. Examples of internal security controls are limit checks and reasonability checks. (AFR 205-16)***
interprocess communication (IPC)	Communication between two different processes using system-supplied constructs; for example, shared files. (MTR-8201)
investigation(s)	The review and analysis of system security features (e.g., the investigation of system control programs using flow charts, assembly listings, and related documentation) to determine the security provided by the operating system. (OPNAVINST 5239.1A; DOD 5200.28M)
isolation	The containment of users and resources in an automated system in such a way that users and processes are separate from one another as well as from the protection controls of the operating system. (AR 380-380; FIPS PUB 39)
items of intrinsic military utility	End items other than those identified in the DOD Militarily Critical Technologies List which transfer to potential adversaries shall be controlled for the following reasons: a. The end product in question could significantly enhance the recipient's military or warmaking capability either because of its technology content or because of the quantity to be sold; or b. The product could be analyzed to reveal U.S. system characteristics and thereby contribute to the development of countermeasures to equivalent U.S. equipment. (DODD 2040.2)

- J -

NOTE: No terms begin with the letter J

- K -

kernel	See SECURITY KERNEL.
kernelized secure operating system (KSOS)	The project to strengthen the UNIX operating system with a security kernel to make it suitable for multilevel operations. (MTR-8201)
key	1) In cryptography, a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) which control the operations of encryption and decryption. (AR 380-380; FIPS PUB 39) 2) A sequence of symbols or their electrical or mechanical equivalents which, in machine or auto-manual cryptosystems, is combined with plain text to produce cipher text. (Often used informally as a synonym for keying material or cryptovariable). (NCSC-9) 3) A sequence of random binary bits used to initially set up and periodically change the encryption/decryption function in a protection equipment for purposes of the encryption, decryption or authentication of information. (NTISSI 3005)

	4) A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt. Also, an element of the arrangement of a crypto-equipment which must be known before encryption or decryption can be carried out. (NACSEM 5201)
key encrypting key	A cryptographic key used for encrypting (and decrypting) data encrypting keys or other key encrypting keys. (FIPS PUB 112)
key generation	The origination of a key or a set of distinct keys. (FIPS PUB 39 AR 380-380)
key loader	An ancillary device used to transfer, store, or load key into a protection equipment. (NTISSI 3005)
key management	Specific manual and computer procedures for the generation, dissemination, replacement, storage archive, and destruction of secret keys that control encryption or authentication processes. (WB)
key management device	A unit that provides for secure electronic distribution of data encryption keys to authorized users. In the DES case, these keys are essentially 56 bits in a 64 bit blocks, therefore, 64 bit blocks can be electronically distributed by a key management (trusted) center. (GAO)
key stream	A sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem, etc, combined with plain test to produce cipher text, to control TRANSEC processes, or to produce other keys. (NTISSI No. 3002)
keyword	Synonymous with PASSWORD.
KVM/370	Kerenlized VM/370. The kernelized version of IBM's VM/370, for S/370 series architecture, being built and verified by System Development Corporation. (MTR-8201)

- L -

label

1) A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object. (CSC-STD-004-85)

2) The marking of an item of information to reflect its classification and its set of categories that represent the sensitivity of the information.

a. Internal Label. The marking of an item of information, to reflect the classification and sensitivity of the information, within the confines of the medium containing the information.

b. External Label. The visible and readable marking on the outside of the medium or the cover of the medium that reflects the classification and sensitivity of the information resident within the medium. (DOE 5637.1)

lattice

A partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound. (DOD 5200.28-STD)

least privilege

This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. (DOD 5200.28-STD)

level I/II/III

See DATA LEVEL.

limited ADP access security mode

An ADP system or network is operating in the limited access security mode when the type of data being processed is categorized as unclassified and requires the implementation of special access controls to restrict the access to the data only to individuals who by their job function have a need to access the data. (OPNAVINST 5239.1A)

limited access	***1) Access to the resources of a system that is limited to only authorized personnel, users, programs, processes, or other systems (computer networks). (AFR 205-16)***
	2) See ACCESS CONTROL.
limited area	A security area for the protection of classified matter where guards, security inspectors, or other internal controls can prevent accesss. See 5632.4 for further information. (DOE 5637.1)
limited exclusion area (LEA)	A room or enclosed area to which security controls have been applied to provide protection to a RED information processing systems equipment and wire lines equivalent to that required for the information transmitted through the system. An LEA must contain a RED equipment area. (NACSIM 5203)
limited protection	1) A form of short-term communications security applied to the electromagnetic or acoustic transmission of unclassified information which warrants protection against simple analysis and easy exploitation but does not require the level of protection needed for classified information. (AR 380-380)
	2) A form of short-term COMSEC protection applied to the electromagnetic or acoustic transmission of national security-related information. (NCSC-9)
linkage	The purposeful combination of data or information from one information system with that from another system in the hope of deriving additional information; in particuiar, the combination of computer files from two or more sources. (FIPS PUB 39; AR 380-380)
link encryption	1) The application of online crypto-operations to a link of a communications system so that all information passing over the link is encrypted in its entirety. (FIPS PUB 39)
	2) End-to-end encryption within each link in a communications network. (FIPS PUB 39)

list oriented	***A computer protection system in which each protected object has a list of all subjects authorized to access it. Compare ticket-oriented. (NCSC-TG-004-88)***
local area network (LAN)	A short-haul data communications system that connects ADP devices in a building or group of buildings within a few square kilometers, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways. (JCS PUB 6-03.7)
local nationals	A non-US citizen who is normally resident in the country in which employed, though not necessarily a citizen of that country, and who is employed by the U.S. Government. (AR 380-380)
lock-and-key protection system	A protection system that involves matching a key or password with a specific access requirement. (FIPS PUB 39; AR 380-380)
logical access control	The use of information-related mechanisms (such as passwords) rather than physical mechanisms for the provision of access control. (WN)
logical completeness measure	A means for assessing the effectiveness and degree to which a set of security and access control mechanisms meets the requirements of security specifications. (AR 380-380; FIPS PUB 39)
logic bomb	***A resident computer program that triggers the perpetration of an unauthorized act when particular states of the system are realized. (NCSC-TG-004-88)***
login/log in	See LOGON.
logoff/log off	Procedure used to terminate connections. (BBD)
logon/log on	1) Procedure used to establish the identity of the user, and the levels of authorization and access permitted. (BBD) 2) Synonymous with LOGIN, SIGNIN, SIGNON.
long-range plan	A written description of the strategy for implementing the Classified Computer Security Program that covers the 5 years beginning at the date of the plan. (DOE 5637.1)

loophole	1) An error of omission or oversight in software or hardware that permits circumventing the access control process. (AR 380-380) 2) Synonymous with FAULT and FLAW.
low water mark	Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the nonhierarchical categories. (DCID 1/16, Sup.)

- M -

magnetic field intensity	The magnetic force required to produce a desired magnetic flux, given as the symbol H (see definition of oersted). (CSC-STD-005-85)
magnetic flux	Lines of force representing a magnetic field. (CSC-STD-005-85)
magnetic flux density	1) The representation of the strength of a magnetic field, given as tie symbol B. (CSC-STD-005-85) 2) See GAUSS.
magnetic remanence	***A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power. (NCSC-TG-004-88)***
magnetic saturation	The condition in which an increase in magnetizing force will produce or result in little or no increase in magnetic flux. (CSC-STD-005-85)
maintenance hook	***Special instructions in software to allow easy maintenance and additional feature development. These are not clearly defined during access for design specification. Hooks frequently allow entry into the code at unusual points or without the usual checks, so they are a serious security risk if they are not removed prior to live implementation. Maintenance hooks are special types of trap doors. (NCSC-TG-004-88)***
major information system	An information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources. (A-130)
malicious logic	Hardware, software, or firmware that is intentionally included in a system for the purpose of causing loss or harm (e.g., Trojan horse). (CSC-STD-005-85; CSC-STD-004-85)

mandatory access control (MAC)

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. (DOD 5200.28-STD; CSC-STD-004-85)

mandatory protection

The result of a system that preserves the sensitivity labels of major data structures in the system and uses them to enforce mandatory access controls. (AFR 205-16)

marking

1) The process of placing a sensitivity designator (e.g., "confidential") with data such that its sensitivity is communicated. Marking is not restricted to the physical placement of a sensitivity designator, as might be done with a rubber stamp, but can involve the use of headers for network messages, special fields in databases, etc. (WB)

2) See LABEL.

masquerading

1) An attempt to gain access to a system by posing as an authorized user. (AR 380-380)

2) Synonymous with MIMICKING and IMPERSONATION.

material

"Material" refers to data processed, stored, or used in, and information produced by an ADP system regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements. (DOD 5200.28M; AR 380-380; ***AFR 205-16***)

media

The peripheral device related physical components used for the storage of data, such as tape reels, floppy diskettes, etc. (WB)

memory bounds

The limits in the range of storage addresses for a protected region in memory.

memory bounds checking

Synonymous with BOUNDS CHECKING. (FIPS PUB 39; AR 380-380)

message authentication code (MAC)

A data-authenticator specifically designed for messages travelling on computer networks, which is implemented as an encryption-generated and (often) truncated quantity that accompanies the message it protects. (WB)

mimicking	Synonymous with IMPERSONATION and MASQUERADING.
minor change to a system of records	A change that does not significantly change the system; that is, does not affect the character or purpose of the system and does not affect the ability of an individual to gain access to his or her record or to any information pertaining to him or her which is contained in the system; e.g., changing the title of the system manager. (A-130)
mission-essential unclassified information	Plain text or machine-encoded unclassified data that, as determined by competent authority (e.g., information owners), has high importance related to accomplishing a DOE mission and requires a degree of protection because unnecessary delays in processing could adversely affect the ability of an owner organization, site, or the Department to accomplish such missions. (DOE 1360.2A)
MLS	The multilevel security formula generator, a flow analysis tool developed at SRI for use with HDM. (MTR-8201)
modem	An electrical device that uses modulation and demodulation circuitry; contraction of modulator-demodulator -- generally used to prepare any information stream for most efficient transmission over an available communication line. (NACSIM 5203)
modes of operation	1) The security environment and method of operating an ADP system or network. (OPNAVINST 5239.1A) ***2) The definition of the security environment and approved methods of operating a system. (NCSC-TG-004-88)***
monitoring	See AUTOMATED SECURITY MONITORING and THREAT MONITORING.
multilevel device	A device that is used in a manner that permits it to simultaneously process data of two or more security levels without risk of compromise. To accomplish this, sensitivity labels are normally stored on the same physical medium and in the same form (i.e., machine-readable or human-readable) as the data being processed. (DOD 5200.28-STD)

multilevel secure

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization. (DOD 5200.28-STD)

multilevel security mode

1) A mode of operation that provides for various levels and categories or compartments of data to be concurrently stored and processed in a system and permits selective access to the material concurrently by users with different security clearances and need-to-know. Internal controls, as well as personnel, physical, and administrative controls, separate users and data on the basis of security clearance. The internal security controls must be thoroughly demonstrated to be effective in preventing unauthorized access to information. (AFR 205-16)

2) A mode of operation in effect when at least some users with access to the system do not have a security clearance or a need-to-know for all classified material in the information system. This mode provides the capability for the concurrent access to and use of the information system by uncleared users and users having different security clearances and need-to-know. The identification, segregation, and control of users and sensitive material on the basis of security clearance, and material classification category, and need-to-know must be essentially under automated control. Operation in this mode should be predicated on a comprehensive demonstration that the internal security controls can effectively prevent malicious attempts to bypass these controls. (AFR 700-10)

3) A mode in which various categories and types of classified materials may be concurrently stored and processed within a system which permits concurrent access by users not cleared for the highest category of information in the system and users having the proper clearances an need-to-know. The separation of personnel and information on the basis of security clearance and need-to-know is accomplished by the operating system and associated system software. (AR 380-380)

4) A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS. (DODD 5200.28)

5) A mode of operation under an operating system (supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP system. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of (a) two or more levels of classified data, or (b) one or more levels of classified data with unclassified data depending upon the constraints placed on the system by the designated approving authority. (DOD 5200.28M)

6) The mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. (CSC-STD-003-85)

7) An operation under an operating system (supervisor or executive program) which provides a capability permitting various categories and types of classified materials to be stored and processed concurrently in an ADP system and permitting selective access to such material concurrently by uncleared users having differing security clearances and need-to-know. Separation of personnel and material on the basis of security clearance and need-to-know is accordingly accomplished by the operating system and associated system software. In a remotely accesses resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and need-to-know. This mode of operation can accommodate the concurrent processing and storage of (1) two or more levels of classified data, or (2) one or more levels of classified data with unclassified data depending upon constraints placed on the system by the DAA. (OPNAVINST 5239.1A)

8) The mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. (NCSC-TG-004-88)

multilevel systems

Systems/networks that incorporate the mode of operation that allows two or more classification levels (inciuding unclassified) of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present. (DOE 5637.1)

multiple access rights terminal

A terminal that may be used by more than one class of users; for example, users with different access rights to data. (FIPS PUB 39; AR 380-380)

multi-user hosts

Host computers that perform processing for more than one user simultaneously. (JCS PUB 6-03.7)

multi-user mode of operation

A mode of operation designed for systems that process sensitive unclassified information in which users may not have a need-to-know for all information processed in the system. this mode is also for microcomputers processing sensitive unclassified information that cannot meet the requirements of the stand-alone mode of operation. (NCSC-TG-004-88)

multi-user security mode	*A mode of operation designed for sensitive unclassified systems in which users may or may have the need-to-know for all sensitive information processed, may simultaneously access the system. (AFR 205-16)*
mutually suspicious	1) Pertaining to the state that exists between interacting processes (subsystems or programs) each of which contains sensitive data and is assumed to be designed so as to extract data from the other and to protect its own data. (FIPS PUB 39; AR 380-380) *2) The state that exists between interacting processes (subsystems or programs) in which neither process can expect the other process to function securely with respect to some property. (NCSC-TG-004-88)*

- N -

nak attack	A penetration technique which capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly and, thus, leaves the system in an unprotected state during such interrupts. (FIPS PUB)
National Computer Security Assessment Program	***A program designed to evaluate the interrelationship of empirical data of computer security infractions and critical systems profiles, while comprehensively incorporating information from the CSTVRP. The assessment builds threat and vulnerability scenarios that are based on a collection of facts from relevant reported cases. Such scenarios are powerful, dramatic, and concise form of representing the value of loss experience analysis. (NCSC-TG-004-88)***
national security	The national defense or foreign relations of the United States. (EO 12356; NACSIM 4004)
National Security Decision Directive 145 (NSDD 145)	Signed by President Reagan on 17 September 1984, this directive is entitled "National Policy on Telecommunications and Automated Information Systems Security." It provides initial objectives, policies, and an organizational structure to guide the conduct of national activities toward safeguarding sytems that process, store, or communicate sensitive information; establishes a mechanism for policy development; and assigns implementation responsibilities.
national security information	Information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and that is so designated. (EO 12356; DOE 5635.1A)
need-to-know	1) A determination made by the processor of sensitive information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the sensitive information in order to perform official tasks or services. (CSC-STD-004-85)

2) The necessity for access to, knowledge of, or possession of certain information required to carry out official duties. Responsibility for determining whether a person's duties require that possession of or access to such information and whether the individual is authorized to receive it rests upon the individual having current possession, knowledge, or control of the information involved and not upon the prospective recipient(s). (OPNAVINST 5239.1A; AR 380-380)

3) The determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, which a prospective recipient has the requirement for access to, knowledge of, or possession of the information to perform official tasks or services. (DODD 5200.28; DOE 5635.1A)

need-to-know violation

The disclosure of classified or other sensitive defense information to a person who is cleared but has no requirement for such information to carry out assigned official duties. (AR 380-380; JCS PUB 6-03.7)

network

1) Two or more systems connected by a communications medium. (AFR 205-16)

2) A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. (DODD 5200.28)

3) A communications medium and all components the transfer of information. Such components may include ADP systems, packet switches, telecommunications controliers, key distribution centers, technical control devices, and other networks. (DOE 5637.1)

4) This is the interconnection of two or more ADP central computer faciiities that provides for the transfer or sharing of ADP resources. The ADP network consists of the central computer facilities, the remote terminals, the interconnecting communication links, the front-end processors, and the telecommunications systems. (OPNAVINST 5239.1A)

5) See COMPUTER NETWORK.

network control system — The computer system that provides the means of collecting and processing information concerning the status of a telecommunications network. (GAO)

network front end — ***A device that implements the necessary network protocols, including security-related protocols, to allow a computer systems to be attached to a network. (NCSC-TG-004-88)***

network manager — Individual responsible for the operation of a network; usually authorizes network membership. (AR 380-380)

network weaving — Network weaving is a technique using different communication networks to gain access to an organization's system. For example, a perpetrator [...] makes a call through AT&T, jumps over to Sprint, then to MCI, and then to Tymnet. The purpose is to avoid detection and trace-backs to the source of the call. (TC)

noise — An unwanted signal which does not convey any information. (NACSEM 5106)

non-discretionary security — The aspect of DOD security policy which restricts access on the basis of security levels. A security level is composed of a read level and a category set restriction. For read-access to an item of information, a user must have a clearance level greater than or equal to the classification of the information, and also have a category clearance which includes all of the access categories specified for the information. (MTR-8201)

nonferrous shielding — An RF shielding material which does not contain iron, and therefore provides less magnetic field attentuation than ferrous shielding. Nonferrous shields, such as aluminum and copper, do provide a high degree of electrostatic shielding. (NACSEM 5203)

non-kernel security-related software (NKSR) — Security-relevant software which is executed in the environment provided by a security kernel, rather than as a part of the kernel. Processes executing NKSR software may or may not require special privilege to override kernel-enforced security rules. (MTR-8201)

nonprocedural language	A formal high-level language for the specification of program modules. Such languages express relations which hold between "input" and "output" values of program variables, without constraining the particular algorithms which implement the change. (MTR-8201)
non-processing input and output devices	A device used to enter information and commands into a host computer and receive information from the host, but performs no processing itself (e.g., simple, memoryless terminals). (JCS PUB 6-03.7)
non-volatile memory	Memory (such as semiconductor memory) that does not lose its memory retention capability when electric power is removed. (JCS PUB 6-03.7)

- O -

object

A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examp1es of objects are: records, blocks, pages, segments, files, directories, directory trees and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc. (DOE 5200.28-STD; ***AFR 205-16***; DCID 1/16, Sup.; ***NCSC-TG-004-88***)

object reuse

The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media must contain no residual data from the previously contained object(s). (DOD 5200.28-STD)

oersted

A unit of measure of the magnetizing force necessary to produce a desired magnetic flux across a surface. (CSC-STD-005-85)

official use only (OUO)

1) A designation identifying unclassified information that may be exempt from mandatory disclosure under the FOIA. (DOE 5635.1A)

2) Synonymous with FOR OFFICIAL USE ONLY.

off-line crypto-operation

1) Encryption or decryption performed separately and at a different time from the transmission or decryption, as by manual or machine crypto-equipments not electrically connected to a signal line. (NCSC-9)

2) See CRYPTO-OPERATION.

one-time passwords

One-time passwords [are] those that are changed after each use [and] are useful when the password is not adequately protected from compromise during login (e.g., the communication line is suspected of being tapped). (FIPS PUB 112)

one-way function

A mathematical process that involves the transformation of data, usually with encryption-related routines, into a quantity that cannot then be used to recover the original data. (WB)

on-line crypto-operation

1) The use of crypto-equipment that is directly connected to a signal line, so that encryption and transmission are accomplished simultaneously. (NCSC-9)

2) See CRYPTO-OPERATION.

open security environment

An environment that includes those systems in which one of the following conditions holds true:

a. Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic.

b. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications. (CSC-STD- 004-85; CSC-STD-003-85)

open storage

The storage of classified information on shelves, in metal containers, locked or unlocked, but not in GSA-approved secure containers, within an accredited facility when such facility is not occupied by authorized personnel. (JCS PUB 6-03.7)

operating system

An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in operating a computer system. Operating systems may perform input or output, accounting, resource allocation, storage assignment tasks, and other system related functions. Synonymous with monitor, executive control program and supervisor. (DOD 5200.28M; ***AFR 205-16***)

operational data security

The protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure during input, processing, or output operations. (AR 380-380)

operations security (OPSEC)	1) The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. (NCSC-9) ***2) An analytical process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations. (NCSC-TG-004-88)***
operations security (OPSEC) indicators	Actions or classified or unclassified information, obtainable by an (OPSEC) adversary, that would result in adversary appreciations, plans, and actions harmful to achieving friendly intentions and preserving friendly military capabilities. (AFR 700-10)
operator of a federal computer system	A federal agency, contractor of a federal agency, or other organization that processes information using a computer system on behalf of the federal government to accomplish a federal function. (PL 100-235)
orange book	***Alternate name for DoD Trusted Computer Security Evaluation Criteria. (NCSC-TG-004-88)***
orange book terminology	The DOD 5200.28-STD (Orange Book) classifies AISs into four broad hierarchical divisions of security protection. Within divisions C and there are further sub-divisions called classes. These classes are also ordered in a hierarchical manner characterized by a set of computer security features they possess (see definition of SECURITY FEATURES). (DODD 5200.28)

orientation	The formal and informal presentations and discussions with the authority responsible for the ADP system which supplements the information in the initial security testing and evaluation (ST&E) request and provides the system evaluators an introduction to the operating environment, the techniques used to provide system security, the identity and location of documentation describing the implementation of system security measures (e.g., O/S modifications, etc.), and the techniques available to demonstrate the effectiveness of such measures in meeting requirements of DoD Directive 5200.28. (DOD 5200.28M)
output	Information that has been exported by a TCB. (DOD 5200.28-STD)
output-only devices	Devices such as printers, connected to a host (directly or via communications devices) that perform no input functions to the host. (JCS PUB 6-03.7)
overt channel	***A path within a computer system or network that is designed for the authorized transfer of data. Compare covert channel. (NCSC-TG-004-88)***
overwrite procedure	1) A procedure to remove or destroy data recorded on ADP magnetic storage media by recording patterns of unclassified data over or on top of the data stored on the media. (CSC-STD-005-85) ***2) A procedure to remove or destroy data recorded on computer storage media by writing patterns of data over or on top of the data stored on the media. See magnetic remanence. (NCSC-TG-004-88)***
overwriting	The obliteration of recorded data by recording different data on the same surface. (FIPS PUB 39; AR 380-380)
owner of data	The individual or group that has responsibility for specific data types, and that is charged with the communication of the need for certain security-related handling procedures to both the users and custodians of this data. (WB)

partitioned security code

1) A mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information handled by the AIS. This encompasses the compartmented mode defined in DCID 1/16. (DODD 5200.28)

2) A mode of operation wherein all personnel have the clearance but not necessarily formal access approval and need-to-know for all information contained in the system. (NCSC-TG-004-88)

passphrase

A sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length. (FIPS PUB 112)

passive wiretapping

The monitoring and/or recording of data while the data is being transmitted over a communications link. (FIPS PUB 39)

password

1) A protected word or string of characters that identifies or authenticates a user for access to a specific system, data set, file, record, and so forth. (***AFR 205-16***; AR 380-380; OPNAVINST 5239.1A)

2) A private character string that is used to authenticate an identity. (DOD 5200.28-STD)

3) A protected word, phrase or string of symbols that is used to authenticate the identity of a user. (DOE 5637.1)

4) A protected word or a string of characters that identifies or authenticates a user, a specific resource, or an access type. Synonymous with KEYWORD. (FIPS PUB 39)

5) A character string used to authenticate an identity. Knowledge of the password and its associated user ID is considered proof of authorization to use the capabilities associated with that user ID. (CSC-STD-002-85)

6) A protected/private character string used to authenticate an identity. (NCSC-TG-004-88)

password dialogue	Synonymous with HANDSHAKING PROCEDURE.
password space	The total number of possible passwords that can be created by a given password generation scheme. (DOE 5637.1)
password system	1) A part of an ADP system that is used to authenticate a user's identity. Assurance of unequivocal identification is based on the user's ability to enter a private password that no one else should know. (CSC-STD-002-85) 2) A system that uses a password or passphrase to authenticate a person's identity or to authorize a person's access to data and which consists of a means for performing one or more of the following password operations: generation, distribution, entry, storage, authentication, replacement, encryption and/or decryption of passwords. (FIPS PUB 112)
penetration	1) The successful unauthorized access to an automated system. (AR 380-380; FIPS PUB 39) 2) The successful and repeatable extraction and identification of recognizable information from a protected data file or data set without any attendant arrests. (OPNAVINST 5239.1; DOD 5200.28M) ***3) The successful act of bypassing the security mechanisms of a system. (NCSC-TG-004-88)***
penetration profile	A delineation of activities required to effect a penetration. (FIPS PUB 39; AR 380-380)
penetration signature	1) The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress. (AR 380-380; FIPS PUB 39) ***2) The characteristics or identifying marks that may be produced by a penetration. (NCSC-TG-004-88)***
penetration study	***A study to determine the feasibility and methods for defeating controls of a system. (NCSC-TG-004-88)***

penetration testing

1) The use of teams consisting of data processing, communications, and security specialists to attempt to penetrate a system for the purpose of identifying any security weaknesses. (AR 380-380)

2) The use of special programmer analyst teams to attempt to penetrate a system for the purpose of identifying any security weaknesses. (FIPS PUB 39)

3) The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under the same constraints applied to ordinary users. (DOD 5200.2S-STD)

4) The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users. (NCSC-TG-004-88)

periods processing

1) Processing various levels of classified information at different times with the system being properly cleared or declassified between periods of processing. For example, an automated system could process Top Secret in the dedicated security mode during one period, both Confidential and Secret in the controlled security mode in a second period, and sensitive unclassified material in a third period. The system is purged of all information and brought to a secure state when transitioning from one period to the next. There should be users during the new period who do not have clearance and need-to-know for information processed during the previous period. (AFR 205-16)

2) The processing of various levels of classified information at distinctly different times with the system being properly cleared or declassified between periods of processing. (AR 380-380)

3) Processing data of a given classification level during a period of time and data of a different classification during a different period of time. Also applies to changing security mode of operation. (OPNAVINST 5239.1A)

4) A manner of operating an AIS in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during the period. (DODD 5200.28)

5) The processing of various levels of sensitive information at distinctly diffferent times. Under periods processing, the system must be purged of all information from one processing period before transitioning to the next when there are different users with differing authorizations. (NCSC-TG-004-88)

permissions — ***A description of the type of authorized interactions a subject can have with an object such as read, write, execute, add, modify, and delete. (AFR 205-16)***

personal data — ***1) Any unique data used about an individual. It is information subject to the Privacy Act of 1974. (AFR 205-16)***

2) Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbols, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. (OPNAVINST 5200.1A)

personal identifier — A data item associated with a specific individual which represents the identity of that individual and may be known by other individuals. (FIPS PUB 112)

personal password	A password that is known by only one person and is used to authenticate that person's identity. (FIPS PUB 112)
personnel screening	A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual. (Guidelines on screening non-federal employees are available from the Office of ADP Management.) (DOE 1360.2A)
personnel security	1) The procedures established to ensure that all personnel who have access to any classified information have the required authorizations, as well as the appropriate clearances. (DOE 5637.1) 2) The procedures established to ensure that all personnel who have access to sensitive defense information have the required authority, as well as appropriate clearances. (AR 380-380; FIPS PUB 39) 3) The procedures established to ensure that each individual has a background which indicated a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access. (OPNAVINST 5239.1A) ***4) The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. (NCSC-TG-004-88)***
phracker	Individual who combines phone "PHReaking" with computer "hACKing." (BBD)
phreak	Individual fascinated by the telephone system (a PHone fREAK. Commonly, an individual who uses his knowledge of the telepnone system to make calls at the expense of another. (BBD)

physical compromise

The compromise of information through loss, theft, capture, recovery by salvage, defection of individuals, unauthorized viewing or photography, or by any other physical means. (NACSIM 5203)

physical control space/physically controlled space (PCS)

1) The spherical space surrounding electronic equipment used to process information under sufficient physical control to stop intercept of compromising emanations. It is usually expressed in meters and can be controlled by fences, guards, patrols, walls, and so forth. The exact method of securing the PCS may vary depending upon resources available. (***AFR 205-16***; OPNAVIST 5239.1A)

2) The space surrounding equipment processing classified information which is under sufficient physical and technical control to preclude a successful hostile intercept attack. (AR 380-380)

physical security

1) Those measures used to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and documents; to safeguard them against espionage, sabotage, damage and theft; and, to reduce the exposure to threats which could result in a disruption or denial of service. (AR 380-380)

2) a. The use of locks, guards, badges, alarms, and similar measures (alone or in combination) to control accesss to the classified ADP system and related equipment.

b. The measures required for the protection of the structures housing the classified ADP system, related equipment, and their contents from espionage, theft, misuse, abuse, or damage by accident, fire, and environmental hazards. (DOE 5637.1)

3) a. The use of locks, guards, badges, and similar administrative measures to control access to the computer and related equipment.

b. The measures required for the protection of the structures housing the computer, related equip-ment and their contents from damage by accident, fire, and environmental hazards. (FIPS PUB 39)

4) The component of COMSEC which results from all physical measures necessary to safeguard COMSEC material and information from access thereto or observation thereof by unauthorized persons. (NCSC-9; JCS PUB 1)

5) Physical security is the protection of a material entity (property) from disruption of its safe and secure state and is concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft.

a. The use of locks, badges, and similar measures to control access to the central computer facility.

b. The measures required for the protection of the structures housing the central computer facility from damage by accident, fire, environmental hazards, loss of utilities, and unauthorized access. (OPNAVINST 5239.1A)

6) The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information. (NCSC-TG-004-88)

piggyback

1) Gaining unauthorized access to a system via another user's legitimate connection. See between-th-lines entry. (NCSC-TG-004-88)

2) See BETWEEN-THE-LINES ENTRY and PIGGY BACK ENTRY.

piggy back entry

Unauthorized access that is gained to an ADP system through another user's legitimate connection. (FIPS PUB 39; AR 380-380)

plaintext	Intelligence-bearing signals which can be interpreted without recourse to any decryption or deciphering process. (NACSEM 5106)
plain text/ plain-text	Intelligible text or signals that have meaning and which can be read or acted upon without the application of any decryption. (FIPS PUB 39; AR 380-380; NACSEM 5103; NACSEM 5201; NACSIM 5203)
policy	Administrative decisions which determine how certain security-related concepts will be interpreted as system requirements. All such policy decisions must eventually be interpreted formally and implemented. (MTR-8201)
power line conduction	Plaintext emanations which are propagated or transmitted over power lines. (NACSEM 5106)
power line modulation	Phase or amplitude variations of the input power current which may be related to the information being processed on a power line. (NACSEM 5106)
Preferred Products List (PPL)	***A list of commercially produced equipments that meet TEMPEST and other requirements prescribed by the National Security Agency. This list is included in the NSA Information Systems Security Products and Services Catalogue, issued quarterly and available through the Government Printing Office. (NCSC-TG-004-88)***
primary distribution	The initial targeted distribution of or access to technical documents authorized by the controlling DOD office. (DODD 5230.24)
principle of least privilege	The granting of the minimum access authorization necessary for the performance of required tasks. (FIPS PUB 39; AR 380-380)
print suppression/ print suppress	To eliminate the printing of characters in order to preserve their secrecy; for example, the characters of a password as it is keyed at the input terminal. (FIPS PUB 39; AR 380-380)
privacy	1) The right of an individual to self-determination as to the degree to which personal information will be shared among other individuals or organizations. This includes the right of individuals and organizations to control the collection, storage, and dissemination of personal or organizational information. (AR 380-380)

2) a. The right of an individual to self-determination as to the degree to which the individual is willing to share with others information about himself that may be compromised by unauthorized exchange of such information among other individuals or organizations.

b. The right of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves. (FIPS PUB 39)

privacy protection

The establishment of appropriate administrative,protection technical, and physical safeguards to ensure the security and confidentiality of data records and to protect both security and confidentiality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom such information is maintained. (FIPS PUB 39)

privacy transformation

Synonymous with ENCRYPTION ALGORITHM

private communication

A communication in which the parties thereto, in the absence of their consent to be monitored for COMSEC purposes, have a reasonable expectation of privacy. (NACSI 4000A)

privileged data

Data not subject to usual rules because of confidentiality imposed by law, such as chaplain, legal, and medical files. (AFR 205-16)

privileged instructions

1) A set of instructions generally executable only when the automated system is operating in the executive state (such as, interrupt handling); special computer instructions designed to control the protection features of an ADP system (such as storage protection features. (AR 380-380; FIPS PUB 39)

privileged instructions

1) A set of instructions generally executable only when the automated system is operating in the executive state (such as, interrupt handling); special computer instructions designed to control the protection features of an ADP system (such as storage protection features. (AR 380-380; FIPS PUB 39)

2) A set of instructions (e.g., interrupt handling or special computer instructions) to control features (such as storage protection features) generally executable only when the automated system is operating in the executive state. (NCSC-TG-004-88)

privileged process

A process that is afforded (by the kernel) some privileges not afforded normal user processes. A typical privilege is the ability to override the security *-property. Privileged processes are trusted. (MTR-8201)

privilege profile

A computer resident record that indicates the resources that a specific user, process, or computer has been explicitly authorized to access. (WB)

privity

A privileged mode of operation wherein all instructions are operative, giving complete and unrestricted control of the system. (AR 380-380; JCS PUB 6-03.7)

procedural security

1) The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide protection for sensitive defense information. (AR 380-380)

2) Synonymous with ADMINISTRATIVE SECURITY.

3) See ADMINISTRATIVE SECURITY. (NCSC-TG-004-88)

procedures

See BACKUP PROCEDURES, HANDSHAKING PROCEDURES, RECOVERY PROCEDURES, and SYSTEM INTEGRITY PROCEDURES.

process

1) A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space. (DOD 5200.28-STD)

2) The active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. A process consists of a unique address space containing its accessible program code and data, a program location for the currently executing instruction, and periodic access to the processor in order to continue. (MTR-8201)

	3) A program in execution. See domain and subject. (NCSC-TG-004-88)
profiles	A detailed security description of the physical structure, equipment components, equipment locations and relationships, and general operating environment of the automated system. (AR 380-380)
property protection area	An area set aside for the protection of property as required by this Order. See DOE 5632.4 for further information. (DOE 5637.1)
proprietary data	***Data is created, used, and marketed by individuals having exclusive legal rights to the data. (AFR 205-16)***
protect as restricted data (PARD)	A handling method for computer-generated numerical data, or related information, which is not readily recognized as classified or unclassified because of the high volume of output and low density of potentially classified data. The above information is designated as PARD because it has not had a sensitivity (classification) review and must be protected under a different set of security rules. (DOE 5637.1; DOE 5635.1A)
protected distribution system (PDS)	1) An approved telecommunications systems to which electromagnetic and physical safeguards have been applied to permit safe electric transmission of unencrypted sensitive information. (AR 380-380) 2) A telecommunications system to which acoustical, electrical, electromagnetic and physical safeguards have been applied to permit its use for secure electrical or optical transmission of unencrypted classified information or sensitive unclassified information. (DOE 5637.1; JCS PUB 6-03.7)

3) An approved wire line and/or fiber optics system to which adequate acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit its use for the transmission of unencrypted classified information. The associated facilities include all equipment and wire lines so safeguarded. Major components are wire lines, and/or fiber optics, subscriber sets, and terminal equipment. Also known as an "approved circuit." The major components are defined as follows:

a. Distribution System. --The metallic wirepaths or fiber optic transmission paths providing interconnection between components of the protected system.

b. Subscriber Sets and End Terminal Equipments. --The complete assembly of equipment, exclusive of interconnecting wire lines, located on the end-user's or customer's premises. This includes such items as telephones, teletypewriters, facsimile data sets, input-output devices, switchboards, patchboards, ana consoles. (NACSIM 5203)

4) A wireline or fiber-optics system which includes adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information. NOTE: A complete PDS includes the subscriber and terminal equipment, as well as the interconnecting lines. (NCSC-9)

5) A telecommunications system to which electromagnetic and physical safeguards have been applied to permit secure transmission of unencrypted classified information, and which has been approved by the department or agency. The associated facilities include all equipment and lines so safeguarded. Major components are lines (wire or fiber optic), subscriber sets, and terminal equipment. Also known as approved circiut. (NACSIM 5203)

protected wireline distribution system

1) A telecommunications system which has been approved by a legally designated authority and to which electromagnetic and physical safeguards have been applied to permit safe electrical transmission of unencrypted sensitive information. Synonymous with approved circuit. (FIPS PUB 39)

2) See PROTECTED DISTRIBUTION SYSTEM.

protection

See DATA-DEPENDENT PROTECTION, FETCH PROTECTION, FILE PROTECTION, LOCK-AND-KEY PROTECTION SYSTEM, and PRIVACY PROTECTION.

protection-critical portions of the trusted computing base

1) Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. (DOD 5200.28-STD)

2) Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects. Their correct operation is essential to the protection of the data on the system. (NCSC-TG-004-88)

protection index

A measure of percieved risk determined from the combination of the clearance level of users and the classification of the data on the classified ADP system. The determination of this index is described on page III-14, paragraph 5. (DOE 5637.1)

protection mechanisms

See SECURITY FEATURES.

protection philosophy

An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination (appropriate to the evaluation class) of formal and informal techniques is used to show that the mechanisms are adequate to enforce the security policy. (DOD 5200.28-STD)

protection ring

1) One of a hierarchy of privileged modes of an ADP system that gives certain access rights to user programs and processes authorized to operate in a given mode. (FIPS PUB 39; AR 380-380)

	2) One of hierarchy of privileged modes of a sysem that gives certain access rights to user programs and processes authorized to operate in a given mode. (NCSC-TG-004-88)
protective measures	Physical, administrative, personnel, and technical security measures which, when applied separately or in combination, are designed to reduce the probability of harm, loss or damage to, or compromise of an unclassified computer system or sensitive and/or mission-essential information. (DOE 1360.2A)
protocols	*A set of rules and formats, semantic and syntactic, that permits entities to exchange information. (NCSC-TG-004-88)*
provably secure operating system (PSOS)	A capability-based operating system structured as a hierarchy of nested abstract machines. PSOS was designed at SRI and the system design utilizes SPECIAL and MLS. (MTR-8201)
pseudo-flaw	An apparent loophole deliberately implanted in an operating system program as a trap for intruders. (FIPS PUB 39; AR 380-380)
public domain	Software acquired from government or non-government sources, often at no charge, when the source takes no responsibility for the inteqrity or maintenance of the software. (JCS PUB 6-03.7; *AFR 205-16*)
Public Law 100-235	*Also known as the Computer Security Act of 1987, this law creates a means for establishing minimum acceptable security practices for improving the security and privacy of sensitive information in federal computer systems. This law assigns to the National Institute of Standards and Technology responsibility for developing standards and guidelines for federal computer systems. The law also requires establishment of security plans by all operators of federal computer systems that contain sensitive information. (NCSC-TG-004-88)*

purge	1) Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is ensurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. (DODD 5200.28) ***2) The removal of sensitive data from an AIS, AIS storage device, or peripheral device with storage capacity, at the end of a processing period. This action is performed in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. After a purge, the medium can be declassified by observing th ereview procedures of the respective agency. Replaces the term*** clear. ***(NCSC-TG-004-88)***
purging	The orderly review of storage and removal of inactive or obsolete data files and the removal of obsolete data by erasure, overwriting of storage, or resetting of registers. (AR 380-380: FIPS PUB 39)
purging magnetic media	***Removing information from a medium so that data scavenging using any known technique or analysis is prevented. This medium can be subsequently declassified upon observing the review and verify procedures of the respective agency. (NCSC-TG-004-88)***

- Q -

NOTE: There are no terms beginning with **"Q"**.

- R -

radiated signal	Electromagnetic or acoustic emissions of undesired signal data which are propagated through space. (NACSEM 5106)
read	A fundamental operation that results only in the flow of information from an object to a subject. (DOD 5200.28-STD)
read access	Permission to read information. (DOD 5200.28-STD)
read-only memory (ROM)	A storage area in which the contents can be read but not altered during normal computer processing. (DOD 5200.28-STD)
real-time reaction	A response to a penetration attempt which is detected and diagnosed in time to prevent the actual penetration. (FISS PUB 39; AR 380-380)
reasonability checks	***Rules describing unacceptable combinations of results. For example, a program predicting weather should not forecast snow with high temperatures. (AFR 205-16)***

recertification

An ongoing reassurance that a previously certified unclassified computer application processing sensitive information has been periodically reviewed, that compliance with established protection policies and procedures remains in effect, and that security risks remain at an acceptable level. (DOE 1360.2A)

recovery

The breaking back of intelligence from a TEMPEST signal. (NACSEM 5106)

recovery procedures

1) The actions necessary to restore a system's computational capability and data files after a system failure or penetration. (FIPS PUB 39; AR 380-380)

2) The actions necessary to restore a system's computational capability and data files after a system failure. (NCSC-TG-004-88)

RED

1) Refers to equipment and wire lines handling nonencrypted, classified information. (AFR 205-16)

2) See RED DESIGNATION.

RED/BLACK concept

1) The concept that electrical and electronic circuits, components, equipment, systems, and so forth, which handle classified plain language information in electric signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to and differentiate between such circuits, components, equipment, systems, and so forth, and the areas in which they are contained. (AR 380-380; JCS PUB 6-03.7)

The concept that telecommunications circuits components, equipment, and systems which handle classified plain-language information in electrical signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). (NCSC-9)

RED conductor

Any conductor, which may or may not be intended to carry RED signals, connected to RED equipment. The RED side of crypto-equipment or the RED side of isolation devices. (NACSEM 5201)

RED designation	A designation applied to telecommunications circuits, components, equipments, and systems which handle classified plain text or other information which requires protection during electrical transmission and to areas in which such information exists. (NCSC-9)
RED equipment area (REA)	The space within an LEA which is designated for installation of RED information processing equipment, power, signal control, ground feeder, and distribution facilities. (NACSIM 5203)
RED signal line	The term used to designate only those lines that intentionally carry RED signals externally to or from the equipment under test. (NACSEM 5201)
reference monitor	A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediated every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base. (MTR-8201)
reference monitor concept	An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. (DOD 5200.28-STD)
reference validation mechanism	***An implementation of the reference monitor concept. A security kernel is a type of reference validatio mechanism. (NCSC-TG-004-88)***
regrade	A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection. An "upgrade" results in a higher classification; a "downgrade" results in a lower classification. (MTR-8201)
reliability	1) The probability of a given automatic system performing its mission adequately for a period of time under the expected operating conditions. (AR 380-380) ***2) The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions. (NCSC-TG-004-88)***

remanence	1) A measure of the magnetic flux density remaining after removal of an applied magnetic force. Can also mean any data remaining on ADP storage media after removal of the power. (CSC-STD-005-85) 2) The residual magnetism that remains on magnetic storage media after degaussing. (FIPS PUB 39; AR 380-380)
remotely accessed resource-sharing computer system	A computer system which includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more users, and which can be entered from terminals located outside the central computer facility. (DOD 5200.28M; AR 380-380)
remote terminal area	Remote computer facilities, peripheral devices, or terminals which are located outside the central computer facility. (AR 380-380; JCS PUB 6-03.7)
residual risk	***The portion of risk that remains after security measures have been applied. (AFR 205-16)***
residue	Data left in storage after processing operations, and before degaussing or rewriting has taken place. (FIPS PUB 39; AR 380-380; ***NCSC-TG-004-88***)
resource	1) Anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time, terminal connect time, amount of directly-addressable memory, disk space, number of I/O requests per minute, etc. (DOD 5200.28-STD) 2) In an ADP system, any function, device, or data collection that may be allocated to users or programs. (FIPS PUB 39; AR 380-380)

resource encapsulation	***The process of ensuring that a resource not be directly accessible by a subject, but that it may be protected so that the reference monitor can properly mediate accesses to it. (NCSC-TG-004-88)***
resource sharing	In an ADP system, the concurrent use of a resource by more than one user, job or program. (FIPS PUB 39; AR 380-380)
resource-sharing computer system	A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and process co-resident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multi-programming, multi-accessing, multi- processing, or concurrent processing. (DOD 5200.28M; AR 380-380)
restricted area	1) Those areas that contain Air Force resources designated a security priority and equates to the term "limited area" as specified in DODD 5210.41 for areas containing nuclear weapons. (AFR 207-1) 2) Any area to which access is subject to special restrictions or controls for reasons of security or safeguarding of property or material. (AR 380-380) ***3) An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. For areas containing nuclear weapons, the term is synonymous with the Department of Defense term, "limited area" as defined in DOD Directive 5210.41. (AFR 205-16)***
restricted data	All data concerning design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the restricted data category pursuant to section 142 of the Atomic Enegry Act of 1954, as amended. (DOE 5635.1A)

review and approval

The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network. (OPNAVINST 5239.1A)

ring back

Procedure where connection to the computer requires two calls. The first, which usually is only one ring, alerts the modem, which will not answer unless the ringing stops for some period of time (typically 30 seconds). This allows the phone to be answered by the computer when appropriate and still be used for normal voice communications. (BBD)

risk

1) The loss potential that exists as the result of threat and vulnerability pairs. Reducing either the threat or the vulnerability reduces the risk. (***AFR 205-16***; AFR 700-10)

2) The uncertainty of loss expressed in terms of probability cf such loss. (AR 380-380)

3) The probability that a hostile entity will successfully exploit a particular telecommunications or COMSEC system for intelligence purposes; its factors are threat and vulnerability. (NCSC-9)

4) A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact. (AFR 205-16)

5) the probability that a particular threat will exploit a particular vulnerability of the system. (NCSC-TG-004-88)

risk analysis

1) A part of risk management that is used to minimize risk by effectively applying security measures commensurate with the relative threats, vulnerabilities, and values of the resources to be protected. The value of the resources includes impact on the organization the automated system supports, and the impact of the loss or unauthorized modification of data. Risk analysis consists of four modules: sensitivity assessment, risk assessment, economic assessment, and security test and evaluation. (AFR 205-16; AFR 700-10)

2) An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. (AR 380-380; FIPS PUB 39)

3) An analysis of system assets and vulnerabilities to estabiish an expected loss from certain events based on established probabilities of occurrence. (DODD 5200.28)

4) The process of identifying security risks, determining their magnitude, and identifying areas needed safeguards. Risk analysis is a part of risk management. Also called risk assessment. (NCSC-TG-004-88)

5) Synonymous with RISK ASSESSMENT.

risk assessment

1) A study of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. Managers use the results of a risk assessment to develop security requirements and specifications. (AFR 205-16)

2) The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. (AR 380-380)

3) An identification of a specific ADP facility's assets, the threats to these assets, and the ADP facility's vulnerability to those tnreats. (DOE 5637.1)

4) An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level. (OPNAVINST 5239.1A)

5) A management tool which provides a systematic approach for determining the relative value and sensitivity of computer installation assets, assessing vulnerabilities, assessing loss expectency or perceived risk exposure levels, assessing existing protection features and additional protection alternatives or acceptance of risks and documenting management decisions. Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and sensitivity/value of the assets to be protected. Risk assessments may vary from an informal review of a small scale microcomputer installation to a more formal and fully documented analysis (i.e., risk analysis) of a large scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches. (DOE 1360.2A)

risk index

1) The difference between the minimum clearance or authorization of AIS users and the maximum sensitivity (e.g., classification and categories) of data processed by the AIS. (DODD 5200.28; CSC-STD-004-85; CSC-STD-004-85)

2) The difference between the minimum clearance or authorization of system users and the maximum sensitivity (e.g., classification and categories of data processed by a system. (NCSC-TG-004-88)

risk management

1) The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA approval. The process facilitates the management of security risks by each level of management throughout the system life cycle. The approval process consists of three elements: risk analysis, certification, and approval. (***AFR 205-16***; AFR 700-10)

2) An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases:

a. Risk assessment, as derived from an evaluation of threats and vulnerabilities.

b. Management decision.

c. Control implementation.

d. Effectiveness review. (AR 380-380)

3) The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation. safeguard implementation, and systems review. (DODD 5200.28)

4) The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NCSC-TG-0004-88)

- S -

safeguarding statement

1) A statement affixed to computer outputs which states the highest classification being processed in an automated system at the time product was produced and requiring its control at that level until a responsible person can determine its true classification. (AR 380-380; JCS PUB 6-03.7)

2) See CAUTION STATEMENT.

safeguards

See SECURITY SAFEGUARDS.

salami technique

In data security, pertains to fraud, spread over a large number of individual transactions, e.g., a program which does not round off figures but diverts the leftovers to a personal account. (MS)

sanitization

The elimination of classified information from an ADP system or media associated with an ADP system to permit the reuse of the ADP system or media at a lower classification level or to permit the release to uncleared personnel or personnel without the proper information access authorizations. (DOE 5637.1)

sanitize

To erase or overwrite classified data stored on magnetic media for the purpose of declassifying the media. (CSC-STD-005-85)

sanitizing

1) The degaussing or overwriting of sensitive information in magnetic or other storage media. (FIPS PUB 39; AR 380-380)

2) Synonymous with SCRUBBING.

scanning

1) Scanning [...] is accomplished by sequentially going through combinations of numbers and letters to look for access to telephone numbers and secret passwords. (TC)

2) See EXHAUSTIVE ATTACK.

scavenging

1) Searching tnrough residue for tie purpose of unauthorized data acquisition. (FIPS PUB 39; AR 380-380)

2) Searching through object residue to acquire unauthorized data. (NCSC-TG-004-88)

scenario analysis	An information systems vulnerability assessment technique in which various possible attack methods are identified and the existing controls are examined in light of their ability to counter such attack methods. (WB)
scientific and technical information (STI)	Communicable knowledge or information resulting from or pertaining to the conduct and management of R&E efforts. STI is used by administrators, managers, scientists, and engineers engaged in scientific and technological efforts and is the basic intellectual resource for and result of such effort. (DODD 3200.12; DODD 5230.24)
scrubbing	Synonymous with SANITIZING.
secure communications processor (SCOMP)	The name given to the Honeywell Level 6 Minicomputer modified to increase its protection capability. Four protection rings were added along with user-initiated input/output to direct-memory access devices. (MTR-8201)
secure configuration management	1) The set of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that such changes will not lead to decreased data security. (AR 380-380; FIPS PUB 39) ***2) The set of procedurs appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's secruity policy. (NCSC-TG-004-88)***
secure operating system	An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system. (FIPS PUB 39; AR 380-380)
secure path	See TRUSTED PATH.
secure state	***1) A known, intended condition achieved through the use of protected or trusted software. In periods processing, the secure state may be reached by booting the controlled copy of the operating system at tne beginning of each session. (AFR 205-16)***

	2) A condition in which no subject can access any object in an unauthorized manner. (NCSC-TG-004-88)
secure subsystem	***A subsystem that contains its own implementaiton of the reference monitor concept for those resources it controls. However, the secure subsystem must depend on other controls and the base operating system for the control of subjects and the more primitive system objects. (NCSC-TG-004-88)***
secure telecommunications and information handling equipment	Equipment designed to secure telecommunications and information handling media by converting information to a form unintelligible to an unauthorized interceptor and by reconverting the information to its original form for authorized recipients. Such equipments, employing a classified cryptographic logic, may be stand-alone crypto-equipments, as well as telecommunications and information handling equipments with integrated or embedded cryptography. (NTISSI 4001)
secure working area	An accredited facility which is used for handling, discussing, or processing sensitive defense information. (AR 380-380)
security	1) The quality or state of being cost-effectively protected from undue losses (e.g., loss of goodwill, monetary loss, loss of ability to continue operations, etc.). (WB) 2) See ADD-ON SECURITY, ADMINISTRATIVE SECURITY, COMMUNICATIONS SECURITY, DATA SECURITY, EMANATION SECURITY, PERSONNEL SECURITY, PHYSICAL SECURITY, PROCEDURAL SECURITY, TELEPROCESSING SECURITY, and TRAFFIC FLOW SECURITY.
security area	A physically defined space containing classified matter (documents or material) subject to physical protection and personnel access controls. See DOE 5632.4 for further information. (DOE 5637.1; DOE 5635.1A)
security audit	An examination of data security procedures and measures for the purpose of evaluating their adequacy and compliance with established policy. (FIPS PUB 39)

security breach	A violation of controls of a particular information system such that information assets or system components are unduly exposed. (WB)
security critical	Security mechanisms which require correct operation to make sure security policy is enforced. The mechanisms may or may not be part of the trusted computing base. (AFR 205-16)
security critical mechanisms	***Those security mechanisms whose correct operation is necessary to ensure that the security policy is enforced. (NCSC-TG-004-88)***
security design review	A review process where the objective is to ascertain that implemented protective measures meet the original overall system design and approved computer application security requirements. The security design review may be a separate activity or an integral function of the overall application system design review activity. (DOE 1360.2A)
security evaluation	***An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process. (NCSC-TG-004-88)***
security fault analysis	***A security analysis, usually performed on hardware at gate level, to determine the security properties of a device when a hardware fault is encountered. (NCSC-TG-004-88)***
security features	1) The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, access control). (DODD 5200.28) ***2) The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards. (NCSC-TG-004-88)***

security filter

1) A set of software routines and techniques employed in ADP systems to prevent automatic forwarding of specified data over unprotected links or to unauthorized persons. (FIPS PUB 39)

2) A trusted subsystem that enforces a security policy on the data that passes through it. (NCSC-TG-004-88)

security flaw

An error of commission or omission in a system that may allow protection mechanisms to be bypassed. (NCSC-TG-004-88)

security flow analysis

1) A type of security analysis performed on a nonprocedural formal system specification which locates potential flows of information between system variables. By assigning security levels to system variables, many indirect information channels can be identified. Security flow analysis defines a security model similar to the access control model (Bell La Padula) but with a finer protection granularity. (MTR-8201)

2) A security analysis performed on a formal system specification that locates potential flows of information within the system. (NCSC-TG-004-88)

security incident

1) Any act or circumstance involving classified information that deviates from the requirements of governing security publications. (AFR 205-10)

2) Any incident involving classified information in which there is a deviation from the requirements of governing security regulations (compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of a security incident). (AR 380-380; JCS PUB 6-03.7)

security inspection

An examination of an ADP system to determine compliance with ADP security policy, procedures, and practices. (OPNAVINST 5239.1A)

security interest

Consists of any of the following which requires special protection: classified matter, special nuclear material, security shipments, secure communications center, sensitive compartmented information facilities, automatic data processing centers, or other systems including classified information, or departmental property. (DOE 5635.1A)

security kernel

1) The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct. (DOD 5200.28-STD)

2) The central part of a computer system (software and hardware) that implements the fundamental security procedures for controlling access to system resources. (FIPS PUB 39)

3) A localized mechanism, composed of hardware and software, that controls the access of users (and processes executing on their behalf) to repositories of information resident in or connected to the system. The correct operation of the kernel along with any associated trusted processes should be sufficient to guarantee enforcement of the constraints on access. TCBs have been implemented using security kernels along with trusted processes. (MTR-8201)

security label

A piece of information that represents the security level of an object. (NCSC-TG-004-88)

security level

The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information. (DOD 5200.28-STD)

security measures

1) Elements of software, firmware, hardware, or procedures included in the system to satisfy security specifications. (AFR 205-16)

2) Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications. (NCSC-TG-004-88)

security mode	1) A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the system. (DODD 5200.28) ***2) A secure mode of operation in which the approving authority accredits a system to operate. Inherent within each of the security modes are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, environmental restrictions, and the range of sensitive information permitted on the system. (NCSC-TG-004-88)***
security module	A shielded and self-contained microcomputer-based device that securely stores security parameters, and that automatically erases such parameters if the device is tampered with. (WB)
security officer	The ADP official, described in OMB Circular A-71, Transmittal Memorandum Number 1 (July 27, 1978), having the designated responsibility for the security of an ADP system. (FIPS PUB 112)
security parameters	The variable secret components that control security processes; examples include passwords, encryption keys, encryption initialization vectors, pseudo-random number generator seeds, and biometric identity parameters. (WB)
security perimeter	***1) The boundary where security controls are in effect ot protect assets. (NCSC-TG-004-88)*** 2) Synonymous with CONTROL ZONE.
security policy	1) The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (DOD 5200.28-STD) ***2) The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. (NCSC-TG-004-88)***

security policy model

1) An informal presentation of a formal security policy model. (DOD 5200.28-STD)

2) A formal presentatoin of the security policy enforced by the system. It must identify the set of rules and practices that regulate how a sysem manages, protects, and distributes sensitive information. See Bell-LaPadula model and formal security policy model. (NCSC-TG-004-88)

3) See BELL LAPADULA MODEL, FORMAL SECURITY POLICY MODEL, POLICY and SECURITY POLICY.

security range

The highest and lowest security levels that are permitted in or on a system, systems component, subsystem or network. (NCSC-TG-004-88)

security relevant event

Any event that attempts to change the security state of the system (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.). (DOD 5200.28-STD)

security requirements

1) Types and levels of protection necessary for equipment, data, information, applications, and facilities. (AFR 205-16)

2) The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (NCSC-TG-004-88)

security requirements baseline

1) A description of minimum requirements provided for a system to maintain an acceptable level of security. The baseline does not necessarily constitute one document but may be an accumulation of the security requirements stated in several documents such as SONs, SOWs, CSRDs. (AFR 205-16)

2) A description of minimum requirements necessary for a system to maintain an acceptable level of security. (NCSC-TG-004-88)

security safeguards	1) The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. (DODD 5200.28) ***2) The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Also called safeguards. (NCSC-TG-004-88)***
security specifications	1) A detailed description of the safeguards required to protect a sensitive application. (A-130) ***2) Detailed descriptions of protection measures required by security requirements. Applicable requirements from Air Force policies, publications, and standards are addressed. (AFR 205-16)*** 3) A detailed description of the countermeasures required to protect an ADP activity or network from unauthorized (accidental or unintentional) disclosure, modification, and destruction of data, or denial of service. (OPNAVINST 5239.1A) ***4) A detailed description of the safeguards required to protect a system. (NCSC-TG-004-88)***
security test and evaluation (ST&E)	1) The process to determine that the system administrative, technical, and physical security measures are adequate; to document and report test findings to appropriate authorities; and to to make recommendations based on test results. ST&E may be an integral part of other tests and evaluations. Managers must ensure changes made to correct one problem do not adversely affect other previously tested security measures. (***AFR 205-16***; OPNAVINST 5239.1A)

	2) An examination and analysis of the security features of an operational automated system to develop evidence upon which an accreditation can be based. (AR 380-380; JCS PUB 6-03.7) ***3) An examination and analysis of the security safeguards of a system as they have been applied in an operational environment ot determine the security posture of the system. (NCSC-TG-004-88)***
security testing	A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See Functional Testing, Penetration Testing, Verification. (DOD 5200.28-STD)
security violation	An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. (WB)
seepage	The accidental flow to unauthorized individuals of data or information, access to which is presumed to be controlled by computer security safeguards. (FIPS PUB 39; AR 380-380)
sensitive	Information contained in the Military Critical Technologies List, information which could be useful to a hostile agent in the development of countermeasures, information which could involve new or high technology, information which could involve key indicators of operational capabilities which could be used by hostile agents to determine operational capabilities, weaknesses, and wartime missions. (AFR 700-10)
sensitive application	An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application. (A-130)

sensitive business data	Data which requires protection under Title 18, USC 1905, and other data whicn by its nature requires controlled distribution or access for reasons other than that it is classified or personal data. Sensitive business data is recognized in the following categories: a. For Official Use Only - Requiring confidentiaiity of information derived from Inspector General, authority, or other investigative activity. b. Financial : Requiring protection to ensure the integrity of funds or other fiscal assets. c. Sensitive Management - Requiring protection to defend against the loss of property, material, or supplies or to defend against the disruption of operations or normal management practices, etc. d. Proprietary - Requiring protection to protect data or information in conformance with a limited rights agreement or which is the exclusive property of a civilian corporation or individual and which is on loan to the government for evaluation or for its proper use in adjudicating contracts. e. Privileged - Requiring protection for conformance with business standards or as required by law. (Example: government developed information involving the award of a contract.) (OPNAVINST 5239.1A)
sensitive compartmented information (SCI)	1) Classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence. (DODD 5200.28)

2) All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of intelligence sources and methods and analytical procedures of foreign intelligence programs. The term does not include restricted data as defined in Section 11, Public Law 585, Atomic Energy Act of 1954, as amended. (DCID 1/16; DCID 1/16, Sup.; NACSIM 5203; DOE 5635.1A)

sensitive compartmented intelligence (SCI)

Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentalization is established. (AR 380-380)

sensitive data

1) Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability to accomplish a mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. (A-130)

2) Data designated by a knowledgeable authority to require protection because its unauthorized disclosure, alteration, loss, or destruction could cause damage. It includes both classified and sensitive unclassified data. (AFR 205-16)

sensitive defense information

Any information which requires a degree of protection and which should not be made generally available. This type of information includes, but is not limited to, that information which must be safeguarded as as to:

a. Prevent damage to national defense and which usually bears a security classification.

b. Assure the individual privacy of U.S. citizens as provided by the Privacy Act of 1974.

c. Maintain the confidentiality for FOUO information derived from the Inspector General, an audit, or other investigative activities such as medical or other jurisprudence or disciplinary information derived from records of doctor/patient or lawyer/client relationships.

d. Protect funds, supplies, and material from theft, fraud, misappropriation, or misuse. This includes asset or resource accounting or systems or operations which are involved in the control and distribution of funds or the processing of information which offers the opportunity to divert economically valuable resources.

e. Protect proprietary information which is the exclusive property of an individual or corporation. This proprietary information may be on loan, leased, or purchased by the government or made available to the government for its proper use, to include evaluating or adjudicating contracts.

f. Protect government-developed privileged information involving the award of contracts.

g. Protect information which the commander considers essential for mission accomplishment. (AR 380-380)

sensitive information

1) Any information which requires a degree of protection and which should not be made generally available. (FIPS PUB 39)

2) Information that, as determined by a competent authority, must be protected because its unautnorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. (DOD 5200.28-STD; CSC-STD-003-85; CSC-STD-004-85)

3) Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act) but which has not been specifically authorized under cirteria established by an executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (PL 100-235)

4) Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy. (NCSC-TG-004-88)

5) See SENSITIVE UNCLASSIFIED INFORMATION.

sensitive nuclear material production information

a. Classified production rate or stockpile quantity information relating to plutonium, tritium, enriched lithium-6 and uranium-235 and -233.

b. Laser separation technology. (DOE 5635.1A)

sensitive software

Any data processing software that could bypass, penetrate, or damage data processing security controls. (AR 380-380)

sensitive unclassified information

1) Plain text or machine-encoded data that, as determined by competent authority (e.g., information owners), has relative sensitivity and requires mandatory protection because of statutory or regulatory restrictions (e.g., unclassified controlled nuclear information, Official Use Only Information, Privacy Act information) or requires a degree of discretionary protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect national or other DOE interests (e.g., program critical information, or controlled scientific and technical information which may include computer codes (computer programs) used to process such information). (DOE 1360.2A)

2) Any information, the loss, misuse, or unauthorized access to, or modification of which, adversely might affect U.S. national interest, the conduct of DOD programs, or the privacy of DOD personnel (e.g., FOIA exempt information and information whose distribution is limited by DODD 5230.24). (DODD 5200.28)

3) Information that requires protection due to the risk and magnitude of harm or loss that could result from unauthorized disclosure, alteration, loss, or destruction. The term includes records about individuals requiring protection under the Privacy Act, proprietary data, information not releasable under the Freedom of Information Act, and DOD and Air Force data that affects the mission. (AFR 205.16)

sensitivity and criticality

A method developed to describe the value of an information system by taking into account the cost, capability, and jeopardy to mission accomplishments or human life associated with the system. (AFR 700-10)

sensitivity and criticality assessment

A study to determine the value or importance of the data or the mission it supports. (AFR 205-16)

sensitivity label

A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions. (DOD 5200.28-STD; DCID 1/16, Sup.)

session

An activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon and session termination (a form of logoff). (DCID 1/16, Sup.)

session security level

The security level of a session is the low water mark of the security levels of: the user, the terminal, a level specified by the user, and the system from which the session originates. (DCID 1/16, Sup.)

shielded enclosure	An area (room or box) specifically designed to attenuate electromagnetic radiation and/or acoustic emanation, which may originate either inside or outside the area. (NACSEM 5201; NACSIM 5203)
short range plan	A documented, tactical (1 year) plan describing the implementation of the Classified Computer Security Program. (DOE 5637.1)
shoulder surfing	The stealing of passwords by watching users sign on to systems at their terminals [...]. (TC)
significant change	A change in an unclassified computer installation which could impact overall processing requirements and conditions or installation security requirements (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability; carrying out major hardware configuration upgrades; operating system changes; making change to the physical installation; or changing installation location). (DOE 1360.2A)
significant computer security incident	1) The occurrence of an event which would be of concern to senior DOE management due to potential for public interest or embarrassment to the organization, or potential for occurring at other DOE sites; these events would include such things as unauthorized access, theft, an interruption to computer service or protective controls, an incident involving damage, a disaster, or discovery of a vulnerability. (DOE 1360.2A) 2) See COMPUTER SECURITY INCIDENT.
significant modification	***Any modification to the facility or system that impacts the operation or affects the security measures of the system. Determination of impact is a subjective evaluation and depends on the environment where the system operates. (AFR 205-16)***
significant risk of telecommunications exploitaiton	Exists (a) when information of high value to an adversary may be handled by the telecommunication system and (b) when there is a high potential threat to or a readily exploitable vulnerability in the system. (NCSC-11)

signin	See LOGON.
signon	See LOGON.
simple security condition	1) A Bell La Paduia security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object. (DOD 5200.28-STD) 2) Synonymous with SIMPLE SECURITY PROPERTY. ***3) See SIMPLE SECURITY PROPERTY. (NCSC-TG-004-88)***
simple security property	***A Bell-LaPadula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object. Also called simple security condition. (NCSC-TG-004-88)***
single integrated operational plan-extremely sensitive information (SIOP-ESI)	A DOD special access program. (DODD 5200.28)
single-level device	A device that is used to process data of a single security level at any one time. Since the device need not be trusted to separate data of different security levels, sensitivity labels do not have to be stored with the data being processed. (DOD 5200.28-STD)
single-user hosts	Host computers (e.g., intelligent terminals) that perform processing for only one user at a time (this does not preclude multiple users over time). (JCS PUB 6-03.7)
smart terminal	A terminal (or communications software) which provides features beyond simply transferring data to and from the system. Typical features are: upload and download, graphics displays, formatted screen displays, etc. (BBD)
softlifting	Illegal copying of licensed software for personal use. (PC/PCIE)

software development methodologies	***Methodologies for specifying and verifying design programs for system development. Each methodology is written for a specific computer language. See Enhanced Hierarchical Development Methodology, Formal Development Methodology, Gypsy Verification Environment and Hierarchical Development Methodology. (NCSC-TG-004-88)***
software interface functions	TCB operations that can be invoked by software. (MTR-8201)
software security	1) Those general purpose (executive, utility, or software development tools) and applications programs, and routines which protect data handled by an ADP system and its resources. (AR 380-380) ***2) General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system. (NCSC-TG-004-88)***
software system test and evaluation process	***A process that plans, develops and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational and interface requirements. (NCSC-TG-004-88)***
special access program(s)	1) Any programs imposing need-to-know or related security requirements or constraints which are beyond those normally provided for the protection of information classified in one of the three security classification designations; i.e., Confidential, Secret, or Top Secret. Such a program includes but is not limited to, special clearance, adjudicative, or investigative requirements, special designation of officials authorized to determine need-to-know, or special lists or briefings of personnel determined to have a need-to-know. SIOP-ESI is an example of a DOD Special Access Program. Other sources of additional access control or other pertinent security requirements, not generally applicable to the same security classification category within DOD include: (a) the Atomic Energy Act of 1954; (b) procedures based on International Treaty requirements; and (c) programs for the collection of foreign intelligence or under the jurisdiction of the National Foreign Intelligence Board or the U.S. Communications Security Board. (OPNAVINST 5239.1A)

2) Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know. (***AFR 205-16***; DOE 5635.1A)

split knowledge

1) The condition under which two or more parties separately have part of the data, that when combined, will yield a security parameter or that will allow them to perform some sensitive function. (WB)

2) The separation of data into two or more parts, each part constantly kept under control of separate authorized individuals or teams, so that no one individual will be knowledgeable of the total data involved. (NCSC-9)

sponsor of data

Synonymous with OWNER OF DATA.

spoofing

1) The deliberate inducment of a user or a resource to take an incorrect action. (AR 380-380; FIPS PUB 39)

2) See MASQUERADING. (NCSC-TG-004-88)

stand alone security mode

A mode of operation in which a microcomputer is not networked with another. May process information of any sensitivity level. It applies only to microcomputers without nonremoveable media. (AFR 205-16)

stand-alone, shared system

A system that is physically and electrically isolated from all other systems, and is intended to be used by more than one person, either simultaneously (e.g., a system with multiple terminals) or serially, with data belonging to one user remaining available to the system while another user is using the system (e.g., a personal computer with nonremovable storage media such as a hard disk). (NCSC-TG-004-88)

stand-alone, single-user system	***A system that is physically and electrically isolated from all other systems, and is intended to be used by more than one person at a time, with no data belonging to other users remainig in the system (e.g., a personal computer with removable storage media such as a floppy disk). (NCSC-TG-004-88)***
star property (*-property)	1) A Bell LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. (DOD 5200.28-STD) 2) Synonymous with CONFINEMENT PROPERTY.
state delta verification system	***A system designed to give high confidence regarding microcode performance by using formulae that represent isolated states of a computation to check proofs concerning the course of that computation. (NCSC-TG-004)***
state variable	***A variable that represents either the state of the system or the state of some system resource. (NCSC-TG-004-88)***
ST&E tools and equipment	Specialized techniques, procedures, criteria, standards, programs, or equipment accepted by qualified ST&E personnel for uniform or standard use in testing and evaluating the secure features of ADP systems or networks. (OPNAVINST 5239.1A; DOD 5200.28M)
storage object	An object that supports both read and write accesses. (DOD 5200.28-STD; DCID 1/16, Sup.)
subject	An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair. (DOD 5200.28-STD; ***AFR 205-16***; DCID 1/16, Sup.; ***NCSC-TG-004-88***)
subject security level	***A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user with which the subject is associated. (NCSC-TG-004-88)***

subject's security level	1) A subject's security level is equal to the security level of the objects to which it has either read only or both read and write access. A subject's security level must always be dominated by the session security level. (DCID 1/16, Sup.) 2) A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user the subject is associated with. (DOD 5200.28-STD)
subscriber sets and end terminal equipments	The complete assembly of equipment, exclusive of interconnecting wire lines, located on the end-user's or customer's premises. This includes such items as telephones, teletypewriters, facsimile data sets, input-output devices, switchboards, patchboards, and consoles. (NACSIM 5203)
supervisor state	Synonym for EXECUTIVE STATE.
survivability	The ability of a system to continue to process critical applications in spite of the fact that it suffered disruptive or damaging events (such as contamination with dust, an earthquake, a bomb, etc.). (WB)
susceptibility	The state or quality of being more exploitable due to a higher level of sensitivity of operations. (AR 380-380)
system	1) An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, controlling or receiving data with a minimum of human intervention. (CSC-STD-003-85; CSC-STD-004-85) ***2) An assembly of computer hardware, software, or firmware configured to classify, sort, calculate, compute, summarize, transmit, store, control, or receive data. A system may consist of a single stand-alone computer or word processor. (AFR 205-16)***

3) See ADP SYSTEM, AUTOMATED INFORMATION SYSTEM, CIPHER SYSTEM, CODE SYSTEM, CONCEALMENT SYSTEM, CRYPTOGRAPHIC SYSTEM, LOCK-AND-KEY PROTECTION SYSTEM, PROTECTED WIRELINE DISTRIBUTION SYSTEM, and SECURE OPERATING SYSTEM.

system development methodologies — ***Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools. (NCSC-TG-004-88)***

system high security mode — 1) A mode of operation used when all personnel with access to the automated system have a security clearance, but not a need-to-know for all the material then contained in the system. A system operates in the system high security mode when the central computer facility and all of its connected peripheral devices and remote terminals are protected according to the requirement for the highest classification of material contained in the system. In this mode, the system design and operation must provide for some internal control of concurrently available classified material in the system on the basis of need-to-know. (***AFR 205-16***; AFR 700-10; OPNAVINST 5239.1A; AR 380-380)

2) The mode of operation in which system hardware/software is only trusted to provide need-to-know protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats, until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and caveats have been affixed. (CSC-STD-003-85)

3) A mode of operation wherein all users having access to the AIS posses a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval. (DODD 5200.28)

system integrity

1) The state that exists when there is complete assurance that under all conditions an automated system is based on the logical correctness and reliability of the operating hardware and software that implement the protection mechanisms, and data soundness. (AR 380-380)

2) The state that exists when there is complete assurance that under all conditions an ADP system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the protection mechanisms, and data integrity. (FIPS PUB 39)

3) The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (NCSC-TG-004-88)

system integrity procedures

1) The procedure established for assuring that the hardware, software, and data in an automated system maintain their state of original integrity. (AR 380-380)

2) The procedure established for assuring that the hardware, software, and data in an ADP system maintain their state of original integrity and are not tampered with by program changes. (FIPS PUB 39)

system low

The lowest security level supported by a system at a particular time or ina particular environment. (NCSC-TG-004-88)

system manager

The ADP official who is responsible for the operation of an ADP system. (FIPS PUB 112)

system security officer (SSO)

1) The person responsible for tne security of an ADP system. The SSO is authorized to act in the "security administrator" role as defined in CSC-STD-001-83. Functions that the SSO is expected to perform include: auditing and changing security characteristics of a user. (CSC-STD-002-85; CSC-STD-005-85)

2) See INFORMATION SYSTEM SECURITY OFFICER.

3) Synonymous with Computer System Security Officer (CSSO).

tamper-indicative seal

A special seal, approved by NSA, that can be used to seal physical objects, such as ADP terminal workstations. The unauthorized removal of such a seal is clearly recognizable. (JCS PUB 6-03.7)

tampering

An unauthorized modification that alters the proper functioning of an equipment or system in a manner that degrades the security or functionality it provides. (NCSC-TG-004-88)

technical attack

An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users. (NCSC-TG-004-88)

technical security

1) The set of hardware, firmware, software and supporting controls that implement (1) security policy, (2) accountability, (3) assurance, and (4) documentation, as defined in CSC-STD-001-83. (GAO)

2) Equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems. (NSDD-145)

technical vulnerability

1) A hardware, firmware or software weakness or design deficiency that leaves an automated information system open to potential exploitation either externally or internally, thereby resulting in risk or compromise of information, alteration of information, or denial of service. Technical vulnerability information, if made available to unauthorized persons, may allow an AIS to be exploited, resulting in potentially serious damage to national security. (DODI 5215.2)

2) A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system. (NCSC-TG-004-88)

technological attack	An attack which can be perpetrated by circumventing or nullifying hardware and software access control mechanisms, rather than by subverting system peronnel or other users. (AR 380-380; FIPS PUB 39)
telecommunications	1) Under this Directive, a general term expressing data transmission between computing systems and remotely located devices via a unit that performs the necessary format conversion and controls the rate of transmission. (DODD 5200.28) 2) Any transmission, emission, or reception of signs, signals, writing, images, sounds or other information by wire, radio, visual, or any electromagnetic systems. (FIPS PUB 39; AR 380-380) 3) The transmission, communication, or processing of information, including the preparation of such information thereof, by electrical, electromagnetic, electromechanical, or electro-optical means. (NCSC-9) 4) The preparation, transmission, communication, or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means. (NSDD-145)
telecommunications and automated information systems security	Protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information. (NSDD-145)
telecommunications system	The devices used to transmit and/or receive communications or process telecommunications, including the preparation of information, therefore; the devices may be electrical, electromagnetic, electromechanical, or electro-optical. (NACSI 4000A)

teleprocessing	1) A form of information processing in which remote terminals access a computer via some type of communications line. (AR 380-380) 2) Pertaining to an information transmission system that combines telecommunications, ADP systems, and man-machine interface equipment for the purpose of interacting and functioning as an integrated whole. (FIPS PUB 39) 3) The overall function of an information transmission system which combines telecommunications, automatic data processing, and man-machine interface equipment and their interaction as an integrated whole. (NCSC-9)
teleprocessing security	The protection that results from measures designed to prevent deliberate, inadvertent, or unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system. (FIPS PUB 39; NCSC-9; AR 380-380)
TEMPEST	1) A short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations" for example TEMPEST tests, TEMPEST inspections. (AFR 700-10; DOE 5637.1; NCSC-9; JCS PUB 6-03.7) 2) TEMPEST is the unclassified name for the studies and investigations of compromising emanations. (AR 380-380) 3) The study and control of spurious electronic signals emitted from ADP equipment. (DOD 5200.28-STD; ***AFR 205-16***) ***4) The study an dcontrol of spurious electronic signals emitted by electrical equipment. (NCSC-TG-004-88)***
terminal identification	1) The means used to establish the unique identification of a terminal by an automated system. (AR 380-380; FIPS PUB 39) ***2) The means used to uniquely identify a terminal to a system. (NCSC-TG-004-88)***

threat

1) The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. Categorize and classify threats as follows:

Categories	Classes
Human	Intentional
	Unintentional
Environmental	Natural
	Fabricated

(AFR 205-16; AFR 700-10)

2) The technical and operational capability of a hostile entity to detect, expioit, or subvert friendly telecommunications and the demonstrated, presumed, or inferred intent of that entity to conduct such activity. (NCSC-9)

3) Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, andlor denial of service. (NCSC-TG-004-88)

4) Any circumstance or event with the potential to cause harm to the ADP system or activity in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the system or activity and not because of any specific weakness. For example, the threat of fire exists at all facilities, regardless of the amount of fire protection available. (OPNAVINST 5239.1A; AR 380-380)

5) Types of computer systems related adverse events (i.e., perils) that may result in losses. Examples are: flooding, sabotage, and fraud. (WB)

threat agent

1) Methods and things used to exploit a vulnerability in an information system, operation, or facility, for example, fire, natural disaster, and so forth. (AFR 700-10; ***AFR 206-16***; AR 380-380)

	2) A method used to exploit a vulnerability in a system, operation, or facility. (NCSC-TG-004-88)
threat analysis	***The examination of all actions and events that might adversely affect a system or operation. (NCSC-TG-004-88)***
threat event	A specific type of threat event, as often specified in a risk analysis procedure. Exampies are: the neighboring river overflows its banks and submerges the adjacent data processing center under ten feet of water, and an ex-employee throws a molotov cocktail into the organization's off-site data storage facility. (WB)
threat monitoring	1) The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data security. (AR 380-380)
	2) The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events which may constitute violations or precipitate incidents involving data privacy matters. (FIPS PUB 39)
	3) The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security. (NCSC-TG-004-88)
threat, postulated	The means through which the hypothesized ability or intent, inferred from related conditions or evidence, threaten to adversely affect an automated system, facility, or operation. (AR 380-380)
ticket-oriented	***A computer protection system in which each subject maintains a list of unforgeable bit patterns, called tickets, one for each object the subject is authorized to access. (NCSC-TG-004-88)***
time bomb/ time-bomb	In computer security, a variant of the Trojan horse in which malicious code is inserted to be triggered later. (MS; JCS PUB 6-03.7)

time-dependent password	A password which is valid only at a certain time of day or during a specified interval of time. (AR 380-380; FIPS PUB 39)
top-level specification (TLS)	A non-procedural description of system behavior at the most abstract level. Typically functional specification that omits all implementation details. (DOD 5200.28-STD)
traffic analysis	1) The study of communications characteristics which are external to the encrypted texts. (NCSC-9) 2) The process of deducing information from the nature of the traffic on a network (message frequency, message length, etc.) rather than having knowledge of the actual data being transmitted. (WB)
traffic flow information	Any information which reveals the presence or absence of a legitimate message within a given time period. (NACSEM 5201)
traffic flow security	1) The protection that results from those features in some crypto-equipment that conceal the presence of valid messages on a communications circuit. This is usually done by causing the circuit to appear busy at all times, or by encrypting the source and destination addresses of valid messages. (FIPS PUB 39; AR 380-380) 2) The capability of certain on-line, machine-cryptosystems to conceal the presence of valid traffic. (NCSC-9)
tranquility	1) A security model rule stating that the security level of an active object cannot change during the period of activity. (MTR-8201) ***2) A security model rule stating that the security level of an object cannot change while the object is being processed by an AIS. (NCSC-TG-004-88)***
trap door	***1) A hidden software or hardware mechanism that responds to a special input which is used to circumvent security controls. (AFR 205-16)***

2) A condition existing in the system software or hardware which can be triggered to subvert the software or hardware security features. Basically, the condition is prompted internally (such as, by a counter, a date or time value, or any specific set of preestablished circumstances) or externally (such as, by a remote terminal or application program input message). (AR 380-380)

3) A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g. special "random" key sequence at a terminal). (DOD 5200.28-STD)

4) A breach created intentionally in an ADP system for the purpose of collecting, altering or destroying data. (FIPS PUB 39)

5) A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner (e.g., special "random" key sequence at a terminal). Software developers often introduce trap doors in their code that enable them to re-enter the system and perform certain functions. (NCSC-TG-004-88)

Trojan horse

1) A program containing hidden code which allows the unauthorized collection, falsification, or destruction of data. (AFR 205-16)

2) A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan horse. (DOD 5200.28-STD)

3) A computer program that is apparently or actually useful and that contains a trap door. (FIPS PUB 39; AR 380-380)

4) A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity. (NCSC-TG-004-88)

trusted computer system

1) A system that employs sufficient hardware and software integrity measures to allow its use for simultaneous processing of multiple levels of classified and/or sensitive information. (AR 380-380; DOD 5200.28-STD; DODD 5225.1)

2) A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information. (NCSC-TG-004)

trusted computing base (TCB)

1) The totality of protection mechanisms within a computer system including hardware, firmware, and software - the combination of which are responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy. (DOD 5200,28-STD; ***AFR 205-16***)

2) The totality of protection mechanisms within a computer system, including hardware firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system adminstrative personnel of parameters (e.g., a user's clearance level) related to the security policy. (NCSC-TG-004-88)

trusted distribution

A trusted method for distributing the TCB hardware, software, and firmware components, both originals and updates, that provides methods for protecting the TCB from modification during distribution and for detection of any changes to the TCB that may occur. (NCSC-TG-004-88)

trusted facility manual

This manual documents the operational requirements, security environment, hardware and software configuration, and interfaces; all security procedures, measures, and features; and, the contingency plans for computer facilities for continued support in case of local disaster. (AFR 205-16)

trusted identification forwarding

1) An identification method used in networks where the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits tne required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user. (CSC-STD-002-85)

2) An identification method used in networks whereby the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user. (NCSC-TG-004-88)

trusted network interface

A special-purpose device placed between the network and other devices using the network. (AFR 205-16)

trusted path

A mechanism by which a person at a terminal can communicate directly with the trusted computing base. This mechanism can only be activated by the person or the trusted computing base and cannot be imitated by untrusted software. (DOD 5200.28-STD)

trusted process

1) A process which can affect system security. It is sometimes but not always endowed with privileges to override kernel-enforced rules. The protection capabilities or characteristics of a trusted process must be reliably demonstrated to comply with stated requirements, through formal verification when possible. Trusted processes are sometimes used to execute NKSR software. (MTR-8201)

	2) A process whose incorrect or malicious execution is capable of violating system security policy. (NCSC-TG-004-88)
trusted products	Products evaluated and approved for inclusion on tne Evaluated Products List (EPL). (DODD 5200.28)
trusted software	*1) The software portion of a TCB that can be relied upon to enforce security policy. (AFR 205-16)* 2) Software, usually affecting system security, that has been certified to perform as specified. Certification may be performed by any organization the accreditor deems appropriate, depending on the situation. (JCS PUB 6-03.7) 3) The software portion of a trusted computing base. (DOD 5200.28-STD) 4) See TRUSTED PROCESS.
trusted system	Employing sufficient integrity measures to allow its use for processing intelligence information involving sensitive intelligence sources and methods (DCID 1/16, Sup.)
twit	User who can not, or will not use the system properly. Reactions to this type of user are usually severe, including denial of access and notification to other SYSOPs in the area. (BBD)
two person integrity (TPI)	A system of storage and handling designed to prohibit access to certain COMSEC keying material, by requiring the presence of at least two formally authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. (NTISSI 3004)
type1 magnetic media	Magnetic media with coercivity factors not exceeding 3005 oersteds. (CSC-STD-005-85)
type2 magnetic media	Magnetic media with coercivity factors exceeding 3005 oersteds, possibly as high as 750 oersteds (also known as high energy media). (CSC-STD-005-85)

type accreditation	Official authorization by the MAJCOM DAA to employ a system in a specified operational environment. This authorization includes a statement of residual risk, outlines the operating environment, and the system's specific use. This accreditation is optional when multiple copies of a system are to be fielded. (***AFR 205-16***; JCS PUB 6-03.7)

- U -

unapproved software

All software that has not been formally identified, evaluated, and examined by competent personnel to ensure that the software performs to exact specifications. (AR 380-380)

unclassified controlled nuclear information (UCNI)

Unclassified information whose unauthorized dissemination is prohibited under section 148 of the Atomic Energy Act. (DOE 5635.1a)

unclassified information

Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse. (DODD 5200.28)

unclassified telecommunications security

That domain of unclassified computer security that is concerned with protecting the point-to-point communication (e.g., input device to computer, computer to computer) of sensitive unclassified information with appropriate cost-effective measures (e.g., data encryption and protected distribution systems). Such communications generally occur via data communication systems, links, and devices such as networks, local area networks, telephone/wire lines, fiber optics, raoio waves/microwaves, and integrated circuits. (DOE 1360.2A)

uncontrolled access area (UAA)

The area external or internal to a facility over which no personnel access controls can be or are exercised. (NACSIM 5203)

unprotect

1) A software program which copies copy protected software. Usually these programs are available before the "protected" product. (BBD)

2) See COPY PROTECTED.

untrusted process

1) A process whose incorrect or malicious execution cannot affect system security. Verification is usually not applied to untrusted processes. (MTR-8201)

2) A process that has not been evaluated or examined for adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms. (NCSC-TG-004-88)

user(s)

1) An organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to the manager or director of the facility or to the same immediate supervisor. (A-130)

2) An individual (person or organization) with direct access to the system or an individual without access who receives output or generates input not reviewed by another. (***AFR 205-16***; AFR 700-10)

3) Any authorized person, office, or staff agency who may use or receive services or products from a computer system. Synonymous with customer. (AR 380-380)

4) Any person who interacts directly with a computer system. (DOD 5200.28-STD)

5) A user is an individual and/or processes operating on his/her/its behalf. (DCID 1/16, Sup.)

6) People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or software or receive output that is not reviewed for content and classification by a responsible individual). (DODD 5200.28)

7) Any individual who is able to operate any equipment that can access the ADP system or input commands to the ADP system or receive output from the ADP system without intervention of an authorized reviewing official. Note that a user may not necessarily be an authorized user of the ADP system. (DOE 5637.1)

8) A person or organization receiving products or services produced by an ADP system either by access to the system or by other means. (OPNAVINST 5239.1A)

user ID	***A unique symbol or character string that is used by a system to identify a specific user. (NCSC-TG-004-88)***
user profile	***Patterns of a user's activity that can be used to detect changes in normal routines. (NCSC-TG-004-88)***
U.S. nongovernmental source	An individual citizen of the United States or a U.S. corporation, association or other organization substantially composed of United States citizens, which is not directly a part of the government (for example, a self-employed individual, consulting firm, licensee, or contractor, excluding active or reserve military personnel, Civil Service employees, and other individuals employed directly by the government); specifically excluded are corporations or associations under foreign ownership, control, and influence. (NCSC-2)

validation

1) The performance of tests and evaluations in order to determine compliance with security specifications and requirements. (FIPS PUB 39)

2) That portion of the development of specialized ST&E, procedures, tools, and equipment needed to establish acceptance for joint usage by one or more DOD components or their contractors. Such action will include, as necessary, final development, evaluation, and testing leading to acceptance, by senior ST&E staff specialists of the three military departments or a defense agency, and approval for joint usage by the appropriate DOD authority. (AR 380-380; DOD 5200.28M; OPNAVINST 5239.1A)

valid password

A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system. (FIPS PUB 112)

verifiable identification forwarding

1) An identification method used in networks where the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user. (DOE 5637.1)

2) See TRUSTED IDENTIFICATION FORWARDING.

verification

1) The documentation of penetration or attempts to penetrate an actual on-line system in support or in contradiction of assumptions developed during system review and analysis. (AR 380-380)

2) The successful testing and documentation of actual on-line system penetration or attempts to penetrate the system in support or in contradiction or assumptions developed during system review and analysis which are to be included in the evaluation report.
(DOD 5200.28M)

3) The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated. (DOD 5200.28-STD)

virtual password

A password computed from a passphrase that meets the requirements of password storage (e.g., 64 bits for DES). (FIPS PUB 112)

virus

1) A variation of Trojan horse. It attaches itself to files or programs with a triggering mechanism (event, time) with a mission to delete files or send data. Protection from a virus is beyond the criteria set forth in DOD Standard 5200.28-STD, DOD Trusted Computer System Evaluation Criteria. (AFR 205-10)

2) A self-propagating Trojan horse, composed of three parts: a mission component, a trigger component and a self-propagating component. (NCSC-TG-004-88)

volatile memory

Memory (such as semiconductor memory) that loses memory retention capability when electric power is removed. (JCS PUB 6-03.7)

vulnerability

1) A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing. (AFR 700-10; AR 380-380)

2) Characteristics of a friendly telecommunications system or cryptosystem which are potentially exploitable by hostile intelligence entities. (NCSC-9)

3) The susceptibility of a particular system to a specific attack, along with the opportunity available to a hostile entity to mount that attack. A vulnerability is always demonstrable but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control. (JCS PUB 6-03.7)

4) A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack. (OPNAVINST 5239.1A)

5) The characteristic of a system which causes it to suffer a definite degradation (inability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. For computers, it is a weakness in automated systems security procedures, administrative controls, and so forth, that could be exploited to gain unauthorized access to information or disrupt critical processing. (AFR 205-16)

6) A weakness in system security procedures, system design, implementation, internal controls, etc., that coul be exploited to violate system security policy. (NCSC-TG-04-88)

vulnerability analysis

The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures. (NCSC-TG-004-88)

vulnerability assessment

1) A review of the susceptibility to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and/or adverse or unfavorable public opinion. (A-123)

2) A measurement of vulnerability which would include:

a. The susceptibility of a particular system to a specific attack.

b. The opportunity available to a threat agent (methods or things which may be used to exploit a vulnerability (such as fire)) to mount that attack. A vulnerability is always demonstrable but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control. (AR 380-380)

3) A review of the susceptibility to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and adverse or unfavorable public opinion. Vulnerability assessments do not identify weaknesses or result in improvements. They are the mechanism with which an organization can determine quickly the potential for losses in its different programs or functions. The schedule of internal control reviews should be based on the results of the vulnerability assessments. (DODD 7040.6)

4) The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation. (NCSC-9)

5) A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack. (NCSC-TG-004-88)

- W -

weapon data

Restricted data or formerly restricted data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices. (DOE 5635.1A)

wiretapping

1) Cutting in on a communications line to get information.

a. Active. The attaching of an unauthorized device, such as a computer terminal, to a communications circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users.

b. Passive. The monitoring and/or recording of data which is being transmitted over a communication link. (AR 380-380)

2) See ACTIVE WIRETAPPING and PASSIVE WIRETAPPING.

work factor

1) An estimate of the effort or time needed to overcome a protective measure by a potential penetrator with specified expertise and resources. (AR 380-380)

2) An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and resources. (FIPS PUB 39)

3) An estimate of the effort or time needed by a potential penetrator with specified expertise and resources to overcome a protective measure. (NCSC-TG-004-88)

write

A fundamental operation that results only in the flow of information from a subject to an object. (DOD 5200.28-STD)

write access

Permission to write an object. (DOD 5200.28-STD)

- X -

NOTE: There are no terms beginning with the letter **"X"**.

- Y -

NOTE: There are no terms beginning with the letter **"Y"**.

- Z -

NOTE: There are no terms beginning with the letter **"Z"**.

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4659

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
September 1991

4. TITLE AND SUBTITLE

Glossary of Computer Security Terminology

5. AUTHOR(S)

Edward Roback, NIST Coordinator

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Glossary of Computer Security Terminology provides a summary of frequently encountered computer and communications security terms and various definitions used by federal agencies for those terms. This glossary does not provide a single definition per term; rather it reflects the variations in use of these terms among federal organizations.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

ADP security, automated information systems security, communications security, computer security, COMSEC, COMPUSEC, INFOSEC

13. AVAILABILITY

X	UNLIMITED
	FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
	ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
X	ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
176

15. PRICE
A09

ELECTRONIC FORM